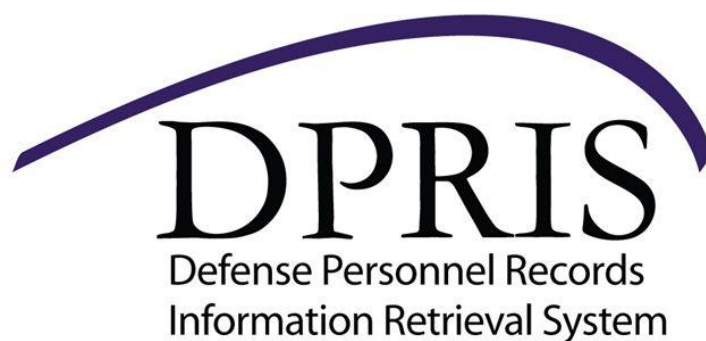


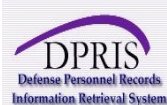


Welcome to DPRIS, *your online gateway to military records!*



Web site User Guide

July 26, 2012



History

Date	Version	Description	Author
07/26/2012	1.0	Initial Release	Booz Allen Hamilton

Change Control for This Document

The DPRIS Web site User Guide is subject to review and update by the DPRIS Program Manager (PM) and DPRIS support team. Review and update will take place when any of the following situations occurs:

- Modifications in response to comments or change requests, if any, received from Personnel and Readiness Information Management (P&R IM)
- Changes in project scope or management processes
- Identification of process-improvement activities that modify risk-management processes, procedures, or practices

This document's Revision History table summarizes changes to the DPRIS Web site User Guide. Each revised plan is subject to the DPRIS Program Management Office (PMO) document review and approval process before becoming final. When the PM has approved and finalized changes, a new version of the DPRIS Web site User Guide will be available for reference by all DPRIS Users.

Table of Contents

1. Introduction.....	1
1.1. Preface.....	1
1.2. Purpose.....	1
1.3. Objective	1
1.4. Recommended Prerequisites	2
1.5. DPRIS User Levels	2
1.6. Personnel Records Available Through DPRIS	3
2. DPRIS Standard Indexing Scheme	4
2.1. Origin of the DPRIS Indexing Scheme	4
2.2. DPRIS Groups and Subgroups	5
3. New User Registration.....	6
3.1. New User registration Home Page	6
3.2. New User Registration Information Page	7
3.3. Privacy and Security Statement.....	8
3.4. Login Method.....	9
3.4.1. User ID and Password Method	9
3.4.2. Common Access Card Method	11
3.5. New User Registration Form.....	14
3.6. Manager Selection Page	15
4. Using DPRIS.....	17
4.1. Logging into DPRIS.....	17
4.1.1. Logging into DPRIS with a User ID and Password.....	17
4.1.2. Logging into DPRIS with a Common Access Card.....	18
4.2. Creating Requests in DPRIS	21
4.2.1. Creating an OMPF Request	22
4.2.2. Creating a JSRRC Request	23
4.3. Viewing Responses	29
4.4. Web-Based DPRIS Reports	31
5. Account Management.....	32
5.1. Changing Your Account Profile.....	34

5.2. Changing Your Password.....	35
5.3. Activating, Deactivating & Rejecting Users	36
5.3.1. Activating New Users	36
5.3.2. Deactivating Users	38
5.3.3. Rejecting a User	40
5.4. Updating User Profiles	41
5.5. Forgotten Passwords	42
5.5.1. Resetting Your Password.....	42
5.5.2. Resetting Another User's Password.....	43
5.6. Reassigning Subordinate DPRIS Users.....	45
6. Information Page	47
7. DPRIS Help	48
8. Conclusion	50
APPENDIX A. Acronyms	51

Table of Figures

Figure 1-1 User Level Permissions.....	2
Figure 1-2 DPRIS User Levels	3
Figure 1-3 Records Available	3
Figure 2-1 Indexing Scheme	4
Figure 3-1 Registering a New User	6
Figure 3-2 New User Registration Information Page	7
Figure 3-3 Privacy and Security Statement	8
Figure 3-4 Login Method Form	9
Figure 3-5 User ID and Password.....	9
Figure 3-6 DPRIS Password Rules	10
Figure 3-7 Common Access Card Method	11
Figure 3-8 Select Certificate	11
Figure 3-9 Select Certificate Prompt	12
Figure 3-10 Security Alert	12
Figure 3-11 PIN Prompt.....	13
Figure 3-12 Certificate Box	13
Figure 3-13 New User Registration Form	14

Figure 3-14 Manager Selection Page	15
Figure 3-15 Manager Information	15
Figure 3-16 Form Submitted	16
Figure 4-1 DPRIS Login	17
Figure 4-2 Select CAC	18
Figure 4-3 Select Certificate	18
Figure 4-4 Security Alert	19
Figure 4-5 Enter PIN	19
Figure 4-6 Certificate ID	20
Figure 4-7 U.S. Government Information System Notification	20
Figure 4-8 View Responses Page	21
Figure 4-9 Create Request Screen	21
Figure 4-10 OMPF Request Form	22
Figure 4-11 JSRRC Request Form	23
Figure 4-12 PTSD Stressor Form	24
Figure 4-13 JSRRC Form	25
Figure 4-14 Agent Orange Claim Form	26
Figure 4-15 Submit Request Form	27
Figure 4-16 Request Submitted	27
Figure 4-17 Response IDs	29
Figure 4-18 List of Available Images	30
Figure 4-19 DD Form 214	30
Figure 4-20 Reports Page	31
Figure 4-21 Web-Based Report	32
Figure 5-1 Account Management	33
Figure 5-2 My Account Profile	34
Figure 5-3 Changing Your Password	35
Figure 5-4 User Accounts	36
Figure 5-5 New User Account	36
Figure 5-6 New User Profile	37
Figure 5-7 Role Assignment	37
Figure 5-8 Deactivating an Active User Account	38
Figure 5-9 Deactivate User Profile	38

Figure 5-10 Deactivate User	39
Figure 5-11 Deactivation Submission.....	39
Figure 5-12 Rejecting a User	40
Figure 5-13 Reject Authorization	40
Figure 5-14 Updating User Profiles	41
Figure 5-15 Invalid Login Attempts	42
Figure 5-16 Forgot Your Password.....	42
Figure 5-17 Forgot Password Prompt	43
Figure 5-18 Resetting Another User's Password.....	43
Figure 5-19 Reset Password Link	44
Figure 5-20 Submit Reset Password	44
Figure 5-21 Reassign Users	45
Figure 5-22 Select User to Reassign	45
Figure 5-23 Select New Manager	46
Figure 5-24 Successful Reassignment	46
Figure 6-1 Information Page	47
Figure 7-1 DPRIS Help.....	48
Figure 7-2 Assistance Form	48
Figure 7-3 Frequently Asked Questions	49

1. INTRODUCTION

1.1. PREFACE

Over the years, the U.S. Services have maintained personnel records in the most efficient and lawful media for the time period. For the greater part of history, records were stored using paper. From the mid-1970s until the 1990s, microfiche was the chosen media to store permanent record information. The next major conversion, digital electronic images, has been adopted by all branches of the Services. This process allows paper to be scanned, indexed with identifiers, and made available for electronic viewing.

The Official Military Personnel File (OMPF) is one of the most important records maintained for individual Service Members. These files contain permanent information for each Service Member and are maintained by the Services in order to administer careers and support certain benefits eligibility. Each of the Services maintains the OMPF information in digital image format. This format enables an authorized individual access to view these images.

The Defense Personnel Records Information Retrieval System (DPRIS) is the primary internet portal supporting external electronic access by authorized government agencies to any of the Services' digital OMPF repositories. DPRIS allows routine authorized Users of OMPF information to obtain copies of the digital images contained in the Services' personnel systems within 48 hours, through a single internet-based interface. Access to the Services' digital OMPF repositories has also been granted to on-site liaison office staff and to agency representatives for walk-in visits to the Service Personnel Command sites.

In the past, information from these records was typically provided via hardcopy, with requests for information and responses to such requests mailed through the U.S. Postal Service. Regardless of the form in which the information is obtained, all Users are required by law to safeguard the information contained in the OMPF. The owners of the OMPF information is required to keep a record pertaining to disclosure of the information, as directed by the Privacy Act of 1974 and Health Insurance Portability and Accountability Act (HIPPA).

The normal means of entry to the DPRIS Web site is through its home page at <https://www.dpris.dod.mil>, which includes a public area open to all internet users. This public area contains descriptive information about DPRIS, as well as links to other related Web sites. However, the primary purpose of DPRIS is to enable authorized routine Users of OMPF information to access digital copies of source documents in a member's or a veteran's file. This functionality is supported within the secure area of the Web site, which is only accessible by pre-authorized Users of government agencies who have logged in via the DPRIS Home Page.

1.2. PURPOSE

This DPRIS Web site User Guide will assist Users of the Web site in ordering digital copies of OMPF documents, reports to which access is authorized, as well as in navigating through the Web site itself (located at <https://www.dpris.dod.mil>). This User Guide also explains, from a typical User's perspective, the DPRIS capabilities and functions encountered while ordering and viewing images through the system. Additional topics include OMPF content, the DPRIS Standard Indexing Scheme, Account Management and troubleshooting for Users.

1.3. OBJECTIVE

The objective of this User Guide is to familiarize Users with the DPRIS Web site and to provide guidance in using DPRIS to submit requests and review responses. In addition, this resource will help Users register for, and manage their accounts, as well as request further assistance if needed.

1.4. RECOMMENDED PREREQUISITES

Each DPRIS User should be familiar with the use of Microsoft Windows and Windows-based applications. In order to initiate requests for and display OMPF images or DPRIS reports, the computer in use must support standard Internet access utilizing standard Microsoft Internet Explorer browser software, including Adobe Reader.

1.5. DPRIS USER LEVELS

There are three levels of DPRIS User groups: Super User, Manager, and User, structured in a top-down, hierarchical approach. Figure 1-1 provides the permissions associated with each of the DPRIS User groups.

TABLE 1: USER LEVEL PERMISSIONS FOR DPRIS			
Permission	Super User	Manager	User
Access the DPRIS website	X	X	X
Request military personnel records	X	X	X
Review retrieved record information	X	X	X
Initiate secure user requests and follow-up messages with OMPF Action Officers	X	X	X
Initiate requests for approved Standard Reports	X	X	X
Manage own personal account information	X	X	X
Maintain oversight of subordinate users	X	X	
Verify and approve/disapprove DPRIS registration requests for subordinate users	X	X	
Reset passwords for subordinate users	X	X	
Assign document and report access for subordinate users	X	X	
Deactivate accounts for subordinate users	X	X	
Review, as warranted, any retrieved record information and follow-up exchanges by subordinate users	X	X	

Figure 1-1 User Level Permissions

As shown in the hierarchical structure in Figure 1-2, Super Users have the roles and responsibilities for all Managers and Users. Managers have the roles and responsibilities for their assigned subordinate Users.

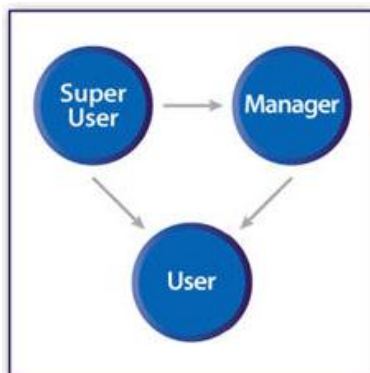


Figure 1-2 DPRIS User Levels

1.6. PERSONNEL RECORDS AVAILABLE THROUGH DPRIS

The OMPF information available through DPRIS have specific dates associated with their branch of Service. Figure 1-3 shows the OMPF information availability dates for each of the Military Services. For example, any Member of the Army who served on or after October 1, 1994 should have OMPF information available via DPRIS. Records for those who were discharged, deceased, released from Active Duty or retired prior to the below dates are likely to be maintained at the National Personnel Records Center (NPRC) www.archives.gov/veterans/evetrecs/. Please refer to the latest Standard Form 180 for more information.

Military Service	Discharged, deceased, released from active duty, or retired on or after
<i>Air Force</i>	<i>October 1, 2004</i>
<i>Army</i>	<i>October 1, 1994</i>
<i>Marine Corps</i>	<i>January 1, 1999</i>
<i>Navy</i>	<i>January 1, 1995</i>

Figure 1-3 Records Available

2. DPRIS STANDARD INDEXING SCHEME

2.1. ORIGIN OF THE DPRIS INDEXING SCHEME

Each of the Services manages their OMPF digital records systems differently. Rather than requiring Users to learn each indexing system, DPRIS has developed a standard index. Each document accessible by DPRIS from the four Service OMPF systems has been mapped to the DPRIS standard indexing scheme. The DPRIS Standard OMPF Document Indexing Scheme is depicted in Figure 2-1. The Figure shows the four major functional document groupings and 26 supporting subgroups.

Service Computation DD-214 / DD-215 Service Verification / Computation Officer Appointment / Termination Enlistments / Extensions Service Acknowledgements / Agreements Discharge / Separation / Retirement Casualty / Death Active / Reserve Orders / Endorsements	Performance Performance / Evaluation Reports Commendatory Items Derogatory Items Sensitive / Restricted Photographs
Professional History Promotion / Advancement / Reduction Service / Military Education / Training Civilian Education / Training Service Status / Changes / Revisions Chronological Assignments History Qualifications / Licenses / Certificates Security Access / Clearance / Screening	Administrative Dependent Support / Eligibility Personal History / Evaluation / Biography Loan / Tuition Assistance / Eligibility Change / Correction / Verification / Proof Medical / Physical / Examinations / Findings Miscellaneous Administrative Documents

Figure 2-1 Indexing Scheme

2.2. DPRIS GROUPS AND SUBGROUPS

All documents in the Service's digital OMPF inventory accessible by DPRIS are assigned to one of the following four major functional groupings:

- Service Computation: Documents that record service entry and exit, length of service, service agreements, appointments, commissions, statements of cumulative service, and other similar time specific data.
- Performance: Documents that record a Service Member's performance including evaluations, fitness reports, effectiveness reports, commendatory or derogatory items, and other performance-specific data.
- Professional History: Documents that record promotions, education, training, chronological listings of assignments, qualifications, and similar historical data.
- Administrative: Documents that record administrative actions or personal information regarding dependents, tuition assistance, medical and dental reports, insurance, and other miscellaneous administrative data.

The Consolidated OMPF Document Mapping Report, published July 24, 1998, assigned each of the individual document types contained in the Services' digital OMPF systems (accessible by DPRIS) to one or more of the DPRIS Standard Index subgroups. Building on this, DPRIS can support standard requests and retrieval of OMPF document images from any of the four OMPF systems using a single functional methodology.

3. NEW USER REGISTRATION

3.1. NEW USER REGISTRATION HOME PAGE

As additional agencies become authorized to retrieve electronic OMPF information via DPRIS, prospective authorized Users within these agencies will need to obtain properly documented approval from their designated Agency DPRIS Manager to become authorized Users of the Web site.

After an agency has completed the pre-negotiated arrangements for its personnel to use DPRIS, individuals within that agency may start their personal registration process via the DPRIS Home Page. To begin the registration process, click the “Register Now” link (Figure 3-1).

The screenshot shows the DPRIS Home Page. At the top, there is a header with the DPRIS logo and the text "Welcome to DPRIS, your online gateway to military records!". Below the header, the page is divided into several sections. On the left, there is a "Login" section with fields for "User ID" and "Password", a "Forgot Your Password?" link, and a "Common Access Card (CAC)" section with a "Select CAC" button and a "Login" button. Below the login section is a "New User Registration" section with the text "(Users from authorized agencies who have NOT registered)" and a "Register Now" button. A red arrow points to the "Register Now" button. To the right of the login section, there is a "Quick Links" section with links to "What is DPRIS?", "Benefits of Using DPRIS", "New User Registration Information", "Access Information", "Individual Veteran Access", and "What's New". Further right, there is a quote from Vice Admiral Daniel L. Cooper (Ret.) about the benefits of DPRIS. At the bottom of the page, there is a footer with links to "Login", "About DPRIS", "Privacy Policy", "Memorandum of Agreement", "FAQs", "Help", "Links", "Site Map", and "Contact Us".

Figure 3-1 Registering a New User

3.2. NEW USER REGISTRATION INFORMATION PAGE

The New User Registration Information page appears. Click the “New User Registration Form” link (Figure 3-2).

DPRIS
Defense Personnel Records
Information Retrieval System

Welcome to DPRIS, your online gateway to military records!

New User Registration Information

New User Registration within an Authorized Agency

If your agency has already been approved as an authorized DPRIS user agency, and you have received permission from your manager to register as a user, please complete the online [New User Registration Form](#). If you have completed the online form and have been granted access to DPRIS, you will be notified by email. If you do not receive approval notification within 48 hours, please contact your Agency Manager.

There are three levels of DPRIS user groups: **Super User**, **Manager**, and **User**, structured in a top-down, hierarchical approach (as shown in Table 1).

Permission	Super User	Manager	User
Access the DPRIS website	X	X	X
Request military personnel records	X	X	X
Review retrieved record information	X	X	X
Initiate secure user requests and follow-up messages with OMPF Action Officers	X	X	X
Initiate requests for approved Standard Reports	X	X	X
Manage own personal account information	X	X	X

Click here to access the [DPRIS Website User Registration Guidance](#), a convenient tool to prepare for self-registration upon notification by a designated agency representative.

DPRISRegistrationG...doc

Show all downloads...

Figure 3-2 New User Registration Information Page

3.3. PRIVACY AND SECURITY STATEMENT

The Privacy and Security Statement page (Figure 3-3) is then displayed. After reading the information presented, click the “Accept” link.

DPRIS
Defense Personnel Records
Information Retrieval System

Welcome to DPRIS, your online gateway to military records!

Privacy and Security Statement

Please read the following DPRIS Privacy and Security Statement. If you agree to comply with the terms and conditions, please select "Accept" to begin the new user registration process.

1. The Office of the Under Secretary of Defense (Personnel and Readiness) provides the Defense Personnel Records Information Retrieval System (DPRIS) to enable the secure retrieval of information from the Service's Official Military Personnel File (OMPF) repositories and narrative data from the Joint Services Records Research Center (JSRRC) for authorized users.
2. Information presented on this Web site is considered public information and may be distributed or copied. Records accessible through DPRIS are protected under the provisions of The Privacy Act of 1974, 5 U.S.C. 552a, as amended. Additionally, as a DoD system, DPRIS must comply with the requirements of DoD Directive 5400.11 and DoD Instruction 5400.11-R.
3. For site management, information is collected for statistical purposes. This government computer system uses software programs to create summary statistics, which are used for such purposes as assessing what information is of most and least interest, determining technical design specifications, and identifying system performance or problem areas.
4. For site security purposes and to ensure that this service remains available to all users, this government computer system employs software programs to monitor network traffic to identify unauthorized attempts to upload information, or otherwise cause damage.
5. Except for authorized law enforcement investigations, no other attempts are made to identify individual users or their usage habits. Raw data logs are used for no other purposes and are scheduled for regular destruction in accordance with National Archives and Records Administration Guidelines (National Archives Schedule 2).
6. Unauthorized attempts to upload information or change information on this service are strictly prohibited and may be punishable under the Computer Fraud and Abuse Act of 1987 and the National Information Infrastructure Protection Act.
7. If you have any questions or comments about the information presented here, please submit an assistance form.

By selecting "Accept," I acknowledge that I have read and understood the DPRIS privacy and security statements, and agree to comply with these policies.

Accept

THIS IS A DEPARTMENT OF DEFENSE COMPUTER SYSTEM. This computer system, including all related equipment, networks, and network devices (specifically including internet access) are provided only for authorized U.S. Government use. DoD computer systems may be monitored for all lawful purposes, including ensuring that their use is authorized, for management of the system, to facilitate protection against unauthorized access, and to verify security procedures, survivability, and operational security. Monitoring includes active attacks by authorized DoD entities to test or verify the security of this system. During monitoring, information may be examined, recorded, copied and used for authorized purposes. All information, including personal information, placed or sent over this system may be monitored. Use of this DoD computer system, authorized or unauthorized, constitutes consent to monitoring of the system. Unauthorized use may subject you to criminal prosecution. Evidence of unauthorized use collected during monitoring may be used for administrative, criminal, or other adverse action. Use of this system constitutes consent to monitoring for these purposes.

[Login](#) [About DPRIS](#) [Privacy Policy](#) [Memorandum of Agreement](#) [FAQs](#) [Help](#) [Site Map](#) [Contact Us](#)

Figure 3-3 Privacy and Security Statement

3.4. LOGIN METHOD

The Login Method Screen (Figure 3-4) is then displayed. Two login choices are presented: User ID and Password Method (Section 3.4.1), and Common Access Card (CAC) method, described in Section 3.4.2.

3.4.1. User ID and Password Method

Select the “User ID and Password” radio button and click “Continue”.

Figure 3-4 Login Method Form

Selecting the User ID and Password Method and clicking “Continue” will bring you to the New User Registration Form show in Figure 3-5.

Figure 3-5 User ID and Password

3.4.1.1. DPRIS Password Rules

To insure security, create a password that adheres to the specific DPRIS Password Rules (Figure 3-6). The Password Rules also ensure integrity of the system.

NOTE: User ID, password, e-mail address and security challenge answer are all case-sensitive in DPRIS.

DPRIS uses an industry standard process for establishing passwords. These rules are called Strong Passwords. The following rules must be adhered to:

- Each password **must** contain
 1. A minimum of eight (8) character
 2. At least one uppercase alphabetical character
Example: A B C D E F G
 3. At least one (1) lower case alphabetical character
Example: a b c d e f g
 4. At least one (1) numeric character
Example: 1 2 3 4 5 6 7 8 9 0
 5. At least one (1) of the following special characters
Example: ! @ # \$ % ^ () - _ = , . : ; ? ' "
- Each password **must NOT:**
 1. Contain a space
Example: US Gov
- The password may not be changed more than once within a 24 hour period.
- The password must be different than the last ten (10) created by the user.

Figure 3-6 DPRIS Password Rules

An example of an acceptable password would be: Dpris5379!

To continue with the User ID and password method, please skip to Section 3.5, “New User Registration Form”.

3.4.2. Common Access Card Method

Select the “Common Access Card” radio button and click “Continue” (Figure 3-7).

Figure 3-7 Common Access Card Method

Click the “Select Certificate” Button (Figure 3-8).

Figure 3-8 Select Certificate

Select your appropriate certificate from the “Select Certificate” prompt and click “Ok” (Figure 3-9).

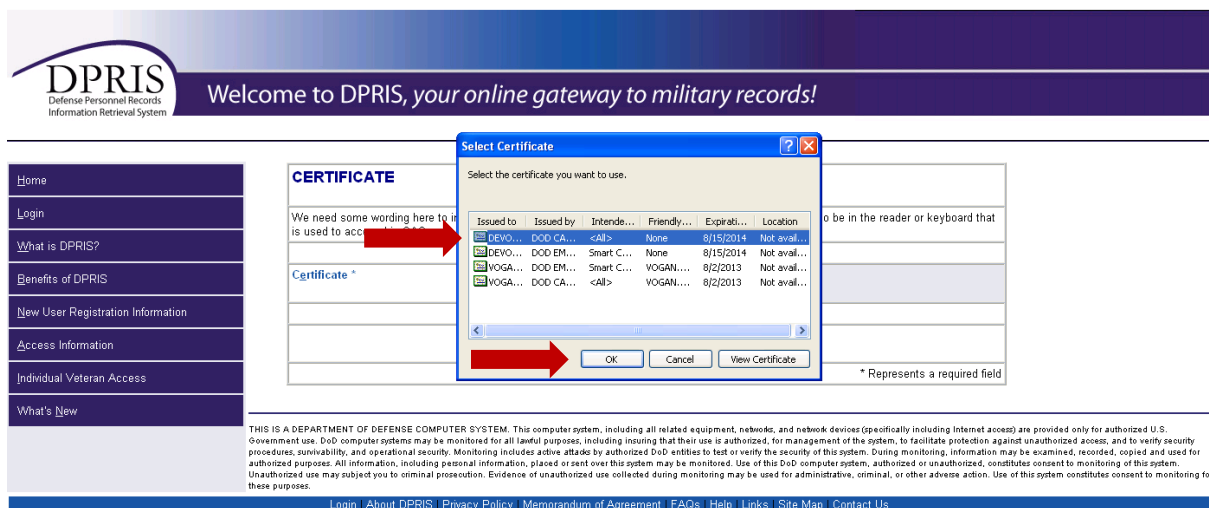


Figure 3-9 Select Certificate Prompt

You will be prompted with a Security Alert. Read the warning and select “Yes” (Figure 3-10).

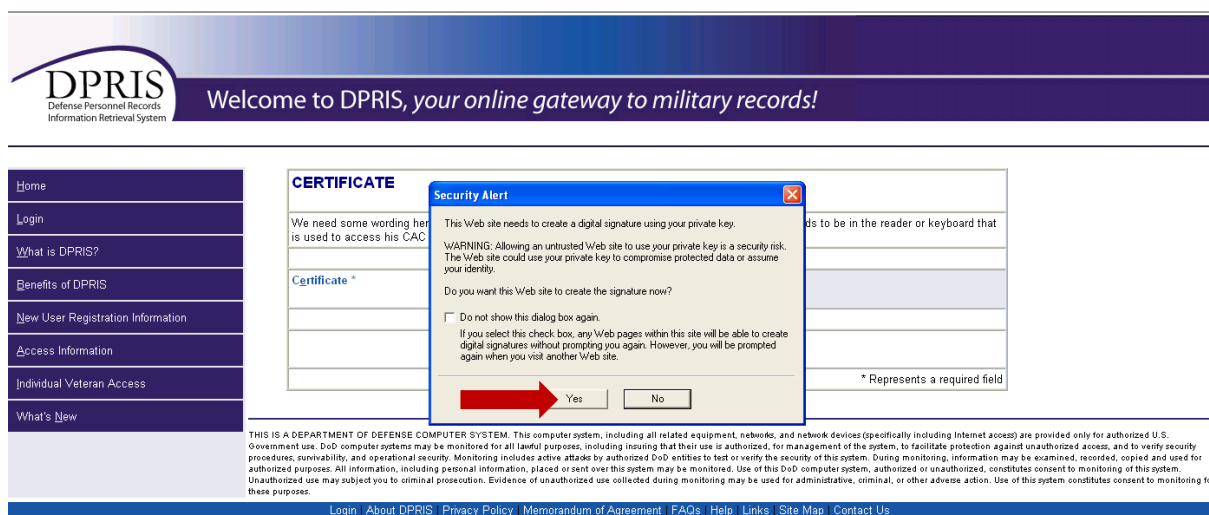


Figure 3-10 Security Alert

Next, you will be prompted to enter your PIN (personal identification number) number into the “ActiveClient Login” prompt and click “OK” (Figure 3-11). Use the PIN number that was set up when you received your Common Access Card.

DPRIS
Defense Personnel Records
Information Retrieval System

Welcome to DPRIS, your online gateway to military records!

CERTIFICATE

We need some wording here to instruct the user that his CAC needs to be accessed and therefore needs to be in the reader or keyboard that is used to access his CAC

Certificate *

Please enter your PIN.

OK Cancel

* Represents a required field

THIS IS A DEPARTMENT OF DEFENSE COMPUTER SYSTEM. This computer system, including all related equipment, networks, and network devices (specifically including Internet access) are provided only for authorized U.S. Government use. DoD computer systems may be monitored for all lawful purposes, including insuring that their use is authorized, for management of the system, to facilitate protection against unauthorized access, and to verify security procedures, survivability, and operational security. Monitoring includes active attacks by authorized DoD entities to test or verify the security of this system. During monitoring, information may be examined, recorded, copied and used for authorized purposes. All information, including personal information, placed or sent over this system may be monitored. Use of this DoD computer system, authorized or unauthorized, constitutes consent to monitoring of this system. Unauthorized use may subject you to criminal prosecution. Evidence of unauthorized use collected during monitoring may be used for administrative, criminal, or other adverse action. Use of this system constitutes consent to monitoring for these purposes.

[Login](#) | [About DPRIS](#) | [Privacy Policy](#) | [Memorandum of Agreement](#) | [FAQs](#) | [Help](#) | [Links](#) | [Site Map](#) | [Contact Us](#)

Figure 3-11 PIN Prompt

DPRIS will bring up your name and certificate information in the certificate box. Click “Continue” (Figure 3-12).

DPRIS
Defense Personnel Records
Information Retrieval System

Welcome to DPRIS, your online gateway to military records!

CERTIFICATE

We need some wording here to instruct the user that his CAC needs to be accessed and therefore needs to be in the reader or keyboard that is used to access his CAC

Certificate *

Click the

Continue Back

* Represents a required field

THIS IS A DEPARTMENT OF DEFENSE COMPUTER SYSTEM. This computer system, including all related equipment, networks, and network devices (specifically including Internet access) are provided only for authorized U.S. Government use. DoD computer systems may be monitored for all lawful purposes, including insuring that their use is authorized, for management of the system, to facilitate protection against unauthorized access, and to verify security procedures, survivability, and operational security. Monitoring includes active attacks by authorized DoD entities to test or verify the security of this system. During monitoring, information may be examined, recorded, copied and used for authorized purposes. All information, including personal information, placed or sent over this system may be monitored. Use of this DoD computer system, authorized or unauthorized, constitutes consent to monitoring of this system. Unauthorized use may subject you to criminal prosecution. Evidence of unauthorized use collected during monitoring may be used for administrative, criminal, or other adverse action. Use of this system constitutes consent to monitoring for these purposes.

[Login](#) | [About DPRIS](#) | [Privacy Policy](#) | [Memorandum of Agreement](#) | [FAQs](#) | [Help](#) | [Links](#) | [Site Map](#) | [Contact Us](#)

Figure 3-12 Certificate Box

You will be brought to the New User Registration Form (Section 3.5).

3.5. NEW USER REGISTRATION FORM


The New User Registration Form (Figure 3-13) is displayed. Input the Agency ID Code provided to you by your Manager or DPRIS point of contact into the Agency ID Code form field. Click on the “Select Manager” link which will bring up a list of Managers to select from (provided a valid Agency ID code is entered).

NEW USER REGISTRATION FORM	
Please complete the online form below to register as a new DPRIS user. Upon completion of all required information fields, click the Submit button at the bottom of the page. An automated email will then be sent to the appropriate manager to approve the new user request. (NOTE: text entered below is case sensitive and will be used each time a user logs into DPRIS.)	
PERSONAL INFORMATION	
First Name *	John
Middle Initial	
Last Name *	Doe
User ID *	John.Doe@va.org
Password *	***** <small>Passwords must contain: at least 8 characters (no spaces), at least one upper case and one lower case alpha, at least one number and one special character. Ex: Moreau200!</small> Click here for a list of password rules.
Confirm Password *	*****
Security Question *	Mothers Maiden Name ▼ <small>Choose a question only you know the answer to and has nothing to do with your password. If you forget your password, we'll verify your identity by asking you this question. The answer you enter should contain only letters (a-z A-Z), numbers (0-9), and these special characters (0@_+,-), and blank spaces.</small>
Security Answer *	***
Email Address *	John.Doe@va.org <small>Please verify that you have entered your correct email address. In order for you to get notifications of the status of your DPRIS requests, and other notifications, your email address needs to be correct.</small>
Confirm Email Address *	John.Doe@va.org
Phone Number *	(901) 555 1597
AGENCY INFORMATION	
Agency ID Code *	[Field] <small>Code exactly as it was given to you. If this code has not yet been supplied to you, please contact your manager before continuing.</small>
Manager *	Select Manager <small>Click the link to get the list of authorized managers for your Agency.</small> <small>The following manager's information will be populated based on the Manager selected. View this information to verify you have selected the correct manager.</small>
Full Agency Name	
Manager's Name	
Manager's Phone	
Manager's Email	
Manager's Office Code or Symbol	
Office Code or Symbol	[Field] <small>Enter an Office Code or Symbol, if your agency uses one. If you are unsure, this field can be left blank now and updated after your account has been activated.</small>
By clicking on the SUBMIT button, you agree to adhere to all provisions of the Privacy Act of 1974 (5 U.S.C. § 552a) and the Health Insurance Portability and Accountability Act of 1996 (HIPAA) (Public Law (P.L.) 104-191.	
<div>Submit</div> <div>Back</div>	
* Represents a required field	
<small> Items, including all related equipment, networks, and network devices (specifically including Internet access) are provided only for authorized U.S. Government use. DoD computer systems may be monitored for all lawful purposes, including ensuring the user use is authorized, for management of the system, to facilitate protection of the security of the system. During monitoring, information may be examined, recorded, copied and used for authorized purposes. All information, including personal information, passed or sent over the system may be monitored. Use of the DoD computer system, authorized or unauthorized, constitutes consent to monitoring of its other otherwise action. Use of the system constitutes consent to monitoring for these purposes. </small>	
Login About DPRIS Privacy Policy Memorandum of Agreement FAQs Help Links Site Map Contact Us	

Figure 3-13 New User Registration Form

3.6. MANAGER SELECTION PAGE

The Manager Selection (Figure 3-14) Page is displayed in. Select the appropriate Manager who will approve the User Registration Form.



DPRIS

Defense Personnel Records
Information Retrieval System

Welcome to DPRIS, your online gateway to military records!

Home

Login

What is DPRIS?

Benefits of DPRIS

New User Registration Information











Access Information

Individual Veteran Access

What's New

Managers for [see the gateway](#)

Please select a name from the list of authorized managers for you Agency. Once a manager has been selected, their information will be added on your registration form.

Name	Office Code	Phone Number
 see the gateway	see the gateway	see the gateway
 see the gateway	see the gateway	see the gateway
 see the gateway	see the gateway	see the gateway
 see the gateway	see the gateway	see the gateway
 see the gateway	see the gateway	see the gateway
 see the gateway	see the gateway	see the gateway
 see the gateway	see the gateway	see the gateway
 see the gateway	see the gateway	see the gateway
 see the gateway	see the gateway	see the gateway
 see the gateway	see the gateway	see the gateway

THIS IS A DEPARTMENT OF DEFENSE COMPUTER SYSTEM. This computer system, including all related equipment, networks, and network devices (specifically including Internet access) are provided only to systems may be monitored for all lawful purposes, including insuring that their use is authorized, for management of the system, to facilitate protection against unauthorized access, and to verify security pro Monitoring includes active attacks by authorized DoD entities to test or verify the security of this system. During monitoring, information may be examined, recorded, copied and used for authorized purposes sent over this system may be monitored. Use of this DoD computer system, authorized or unauthorized, constitutes consent to monitoring of this system. Unauthorized use may subject you to criminal prosec monitoring may be used for administrative, criminal, or other adverse action. Use of this system constitutes consent to monitoring for these purposes.

[Login](#)
[About DPRIS](#)
[Privacy Policy](#)
[Memorandum of Agreement](#)
[FAQs](#)
[Help](#)
[Links](#)
[Site Map](#)
[Contact Us](#)

Figure 3-14 Manager Selection Page

The Manager information will auto-populate into the appropriate fields. To submit the form, click the “Submit” link (Figure 3-15).


Email Address *	John.Doe@va.org Please verify that you have entered your correct email address. In order for you to get notifications of the status of your DPRIS requests, and other notifications, your email address needs to be correct.
Confirm Email Address *	John.Doe@va.org
Phone Number *	() - -
AGENCY INFORMATION	
Agency ID Code *	1 Enter the Agency ID Code exactly as it was given to you. If this code has not yet been supplied to you, please contact your manager before continuing.
Manager *	Change Manager Click the link to get the list of authorized managers for your Agency. The following manager's information will be populated based on the Manager selected. View this information to verify you have selected the correct manager.
Full Agency Name	Booz Allen Hamilton
Manager's Name	D
Manager's Phone	() - -
Manager's Email	ti
Manager's Office Code or Symbol	BAH
Office Code or Symbol	Enter an Office Code or Symbol, if your agency uses one. If you are unsure, this field can be left blank now and updated after your account has been activated.
By clicking on the SUBMIT button, you agree to adhere to all provisions of the Privacy Act of 1974 (5 U.S.C. § 552a) and the Health Insurance Portability and Accountability Act of 1996 (HIPAA) (Public Law (P.L.) 104-191.	
<div>  <div>Submit</div> <div>Back</div> </div>	
* Represents a required field	

Figure 3-15 Manager Information

The Your information was submitted page (Figure 3-16) will appear. This submission will notify the Manager a New User Registration Form has been submitted for approval. Once the Manager approves the account, you will be ready to login and begin using DPRIS.

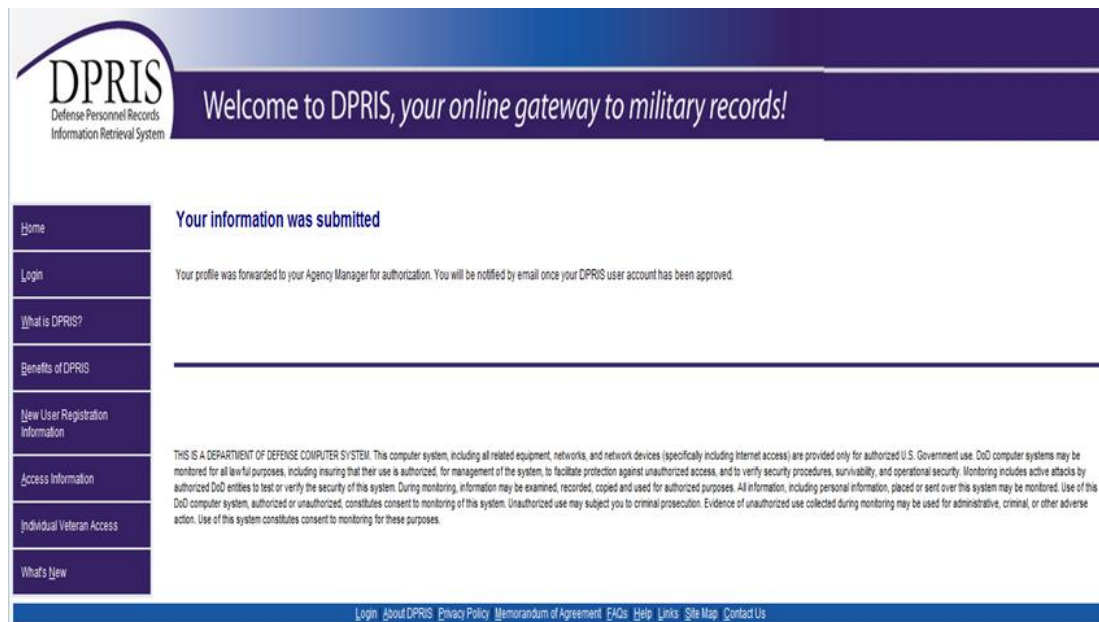


Figure 3-16 Form Submitted

4. USING DPRIS

4.1. LOGGING INTO DPRIS

Two login choices are presented: User ID and Password Method, described in Section 4.1.1, or Common Access Card (CAC) method (4.1.2).

4.1.1. Logging into DPRIS with a User ID and Password

To login with your DPRIS User ID and password, go to the DPRIS Home Page www.dpris.dod.mil, enter your User ID and Password (case-sensitive – must be exact) into the appropriate fields and click “Login” (Figure 4-1).

DPRIS
Defense Personnel Records
Information Retrieval System

Welcome to DPRIS, your online gateway to military records!

Login

User ID
(User ID is case sensitive)
JohnDoe

Password
(Password is case sensitive)

[Forgot Your Password?](#)

Common Access Card (CAC)
(Click CAC button to use your CAC)
Select CAC

Login

New User Registration
(Users from authorized agencies who have NOT registered)
Register Now

DPRIS provides a conduit for the secure electronic retrieval of document images and computable data from the Service's Official Military Personnel File (OMPF) repositories, and narrative data from the Joint Services Records Research Center (JSRRC), in response to requests initiated by veterans and authorized and approved government agency users.

Personal and Readiness Information Management (PRIM), Office of the Under Secretary of Defense (Personnel and Readiness) (OUSD (P&R)), has developed DPRIS, as a single enterprise gateway, to provide access to vital military personnel information on demand and in near real-time through secure system-to-system interfaces and Web access by employing leading edge technologies, including all aspects of information assurance.

Quick Links

- What is DPRIS?
- Benefits of Using DPRIS
- New User Registration Information
- Access Information
- Individual Veteran Access
- What's New

Last Updated 02/16/2011

// DPRIS has greatly improved our ability to gain access to personnel information needed to support the people who matter most — our veterans. Getting these records used to take several months — now, for the veterans who left Service in the last 10 years, we can get the personnel records in hours.

Vice Admiral Daniel L. Cooper (Ret.)
Former Under Secretary for Benefits,
Department of Veterans Affairs

THIS IS A DEPARTMENT OF DEFENSE COMPUTER SYSTEM. This computer system, including all related equipment, networks, and network devices (specifically including Internet access) are provided only for authorized U.S. Government use. DoD computer systems may be monitored for all lawful purposes, including ensuring that their use is authorized, for management of the system, to facilitate protection against unauthorized access, and to verify security procedures, survivability, and operational security. Monitoring includes active efforts by authorized DoD entities to test or verify the security of this system. During monitoring, information may be examined, recorded, copied and used for authorized purposes. All information, including personal information, passed or sent over this system may be monitored. Use of this DoD computer system, authorized or unauthorized, constitutes consent to monitoring of this system. Unauthorized use may subject you to criminal prosecution. Evidence of unauthorized use collected during monitoring may be used for administrative, criminal, or other adverse action. Use of this system constitutes consent to monitoring for these purposes.

[Login](#) [About DPRIS](#) [Privacy Policy](#) [Maintenance of Agreement](#) [FAQs](#) [Help](#) [Links](#) [Site Map](#) [Contact Us](#)

Figure 4-1 DPRIS Login

After clicking “Login” you will be brought to the “U.S. Government System Notification” Page. To continue with the User ID and password login method, please skip forward to Figure 4-7.

4.1.2. Logging into DPRIS with a Common Access Card

To login with your Common Access Card, first insert your CAC into your computer's card reader. From the DPRIS Home screen click the "Select CAC" button (Figure 4-2).

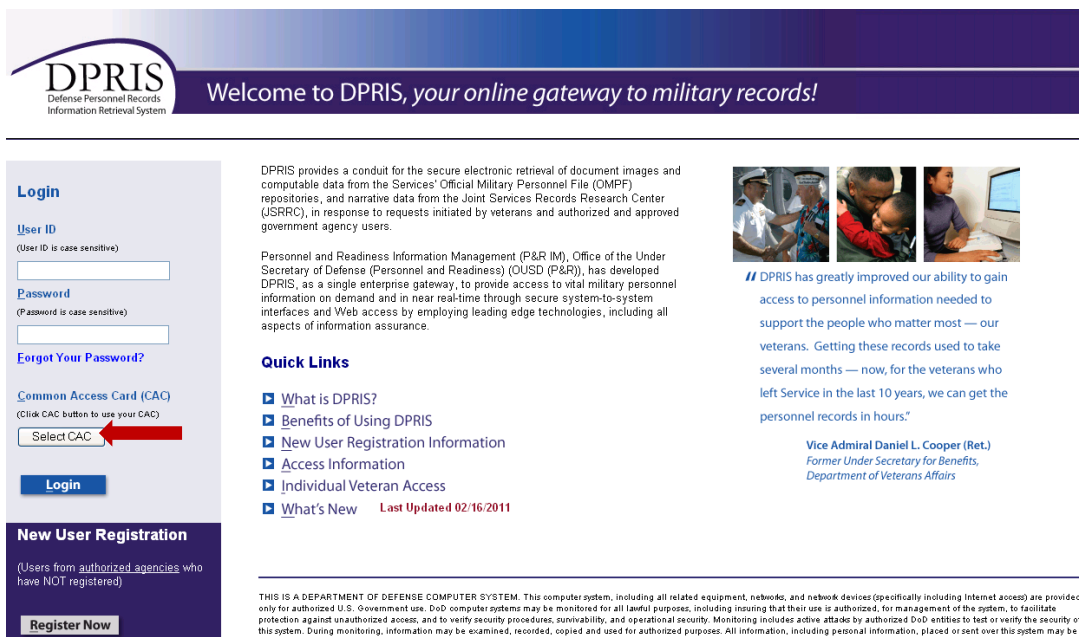


Figure 4-2 Select CAC

You will be prompted to select your certificate from the "Select Certificate" window (Figure 4-3). Select the appropriate certificate.

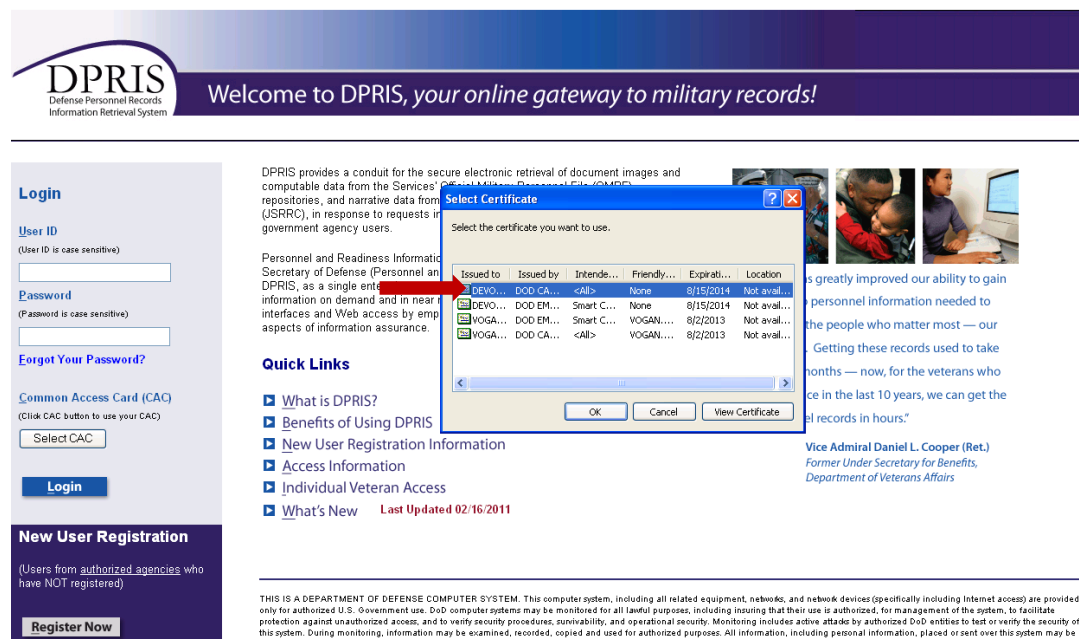


Figure 4-3 Select Certificate

You will be prompted with a Security Alert. Read the warning and select “Yes” (Figure 4-4).

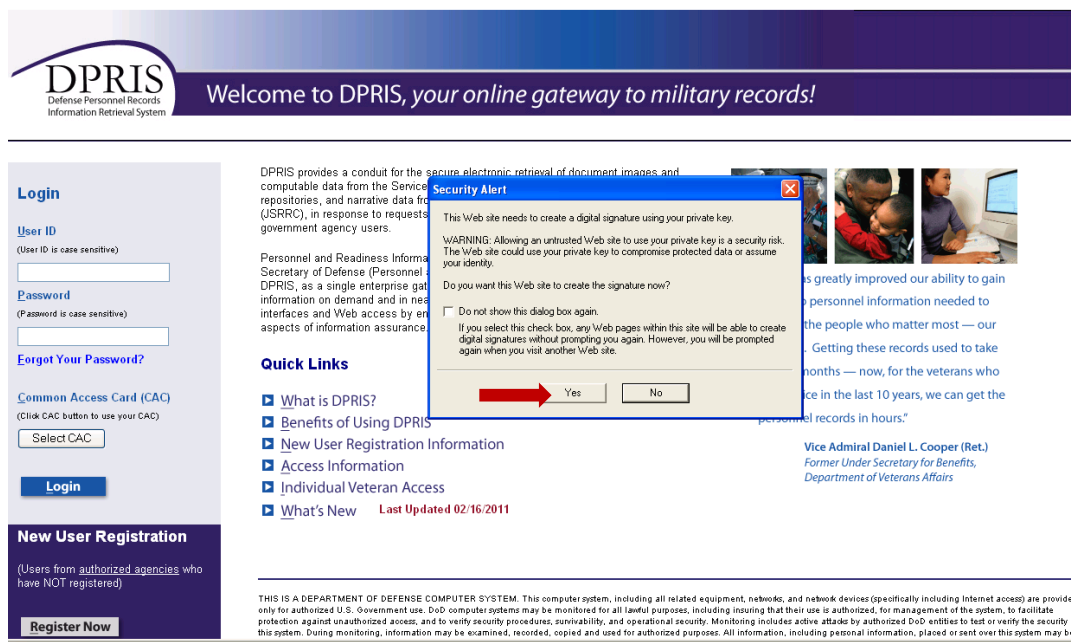


Figure 4-4 Security Alert

You will then be prompted to enter your Common Access Card PIN. Enter your PIN and select “OK” (Figure 4-5).

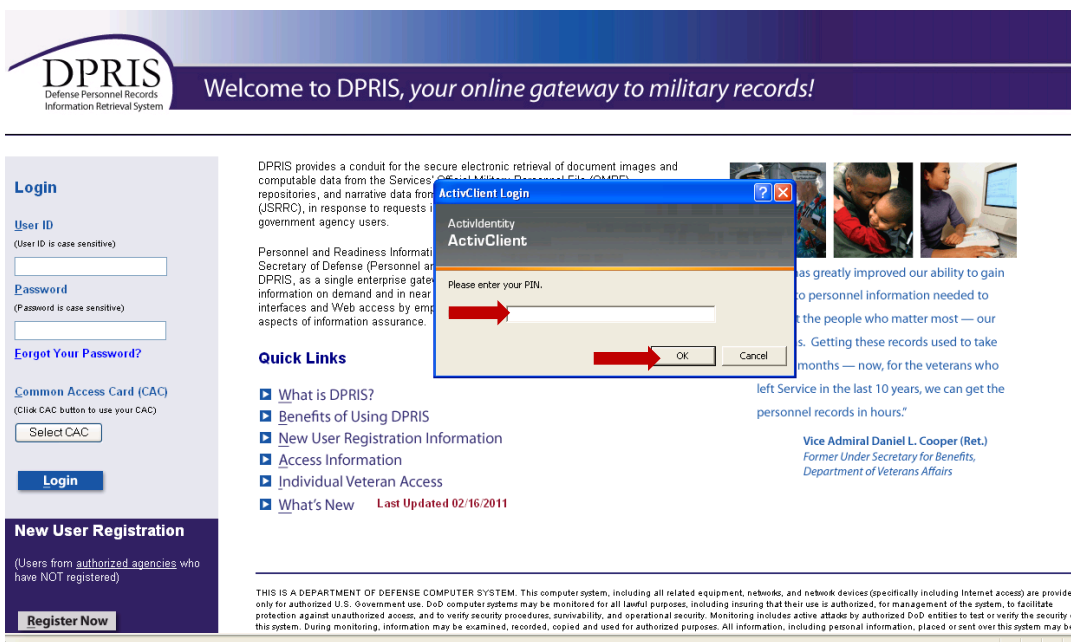


Figure 4-5 Enter PIN

Your User name and certificate number will now appear where the “Select CAC” button was. Click “Login” to continue (Figure 4-6).

Figure 4-6 Certificate ID

The U.S. Government Information System Notification page is displayed. After reading the information, click the “Accept” link (Figure 4-7).

Figure 4-7 U.S. Government Information System Notification

You are now logged into DPRIS.

4.2. CREATING REQUESTS IN DPRIS

The View Responses page (also the default page) (Figure 4-8) is displayed once you are logged into DPRIS. From this page, you can create new requests for images from a Service's OMPF repository or for information from the Joint Services Records Research Center (JSRRC). Click the "Create Request" link to begin the request process.

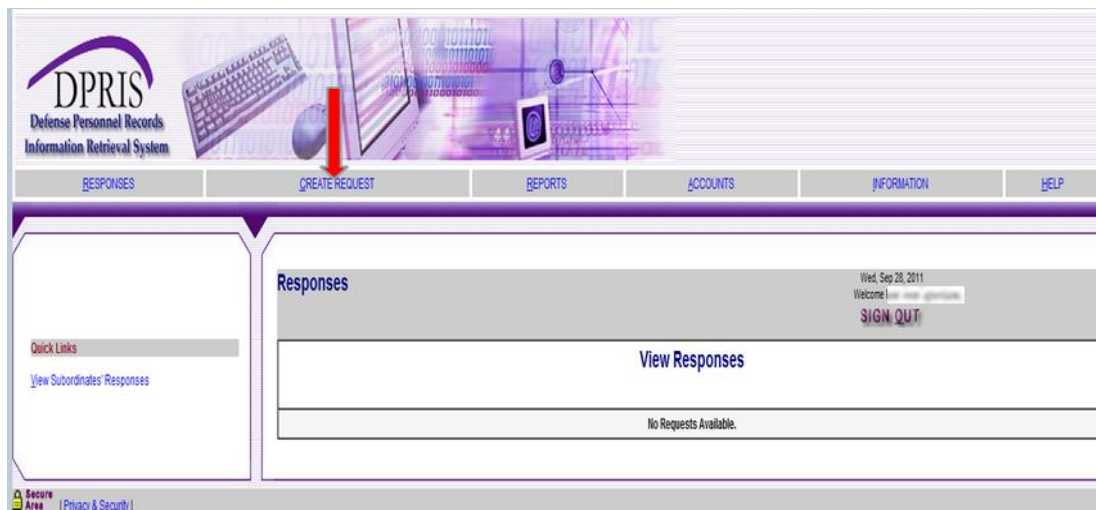


Figure 4-8 View Responses Page

The Create Request page (Figure 4-9) is displayed with a choice to create an OMPF request or, if a User is authorized, to create a JSRRC Request. If a User is not authorized to create a JSRRC Request, that option will not appear.

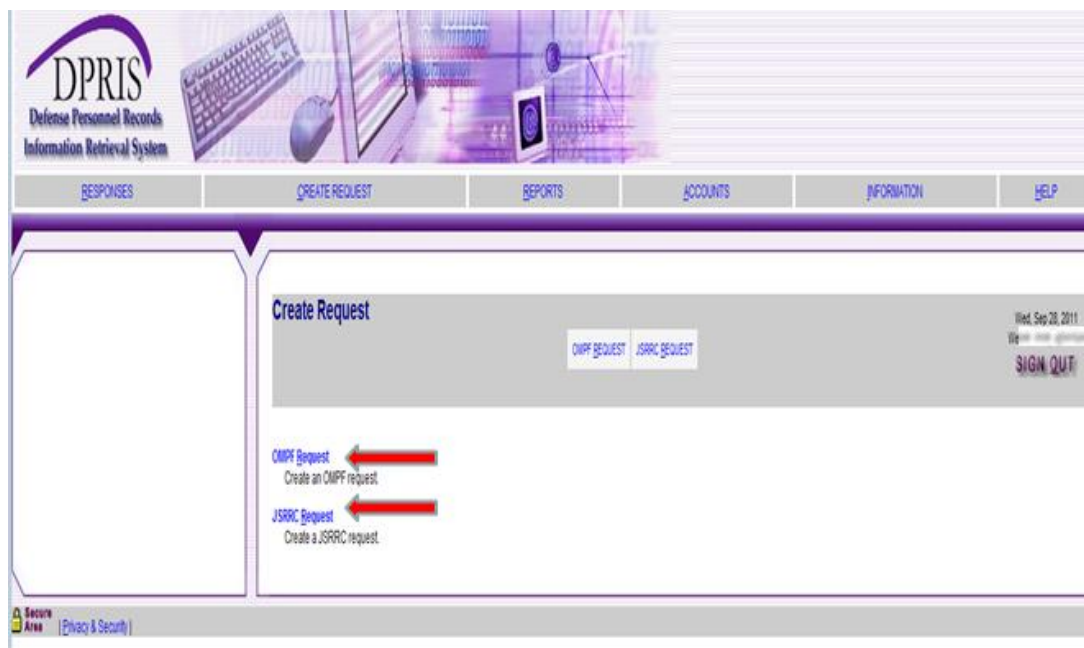


Figure 4-9 Create Request Screen

4.2.1. Creating an OMPF Request

Clicking on the “Create an OMPF request” link from the Create Request Screen (Figure 4-9) will bring you to the OMPF Request Form (Figure 4-10). Fill in the personal information (Full Name and Social Security Number) of the individual you are requesting records for, and select the appropriate OMPF systems(s) to be queried. Make your selections from the document index and click “Submit”.

Create Request

OMPF REQUEST FORM

(*) - Required Fields

PERSONNEL INFORMATION

Social Security Number *

First Name *

Last Name *

OMPF Systems to be queried *

☐ Air Force
☒ Army
☐ Marine Corps
☐ Navy

DOCUMENT INDEX

<input checked="" type="checkbox"/> Service Computation Group SC1 <input checked="" type="checkbox"/> DD214 SC2 <input checked="" type="checkbox"/> Service Verification/Computation SC3 <input checked="" type="checkbox"/> Officer App/ Termination SC4 <input checked="" type="checkbox"/> Enlistment/Extensions SC5 <input checked="" type="checkbox"/> Service Acknowledgement/Lgt SC6 <input checked="" type="checkbox"/> Discharge/ Separation/Ret SC7 <input checked="" type="checkbox"/> Casualty/Death SC8 <input checked="" type="checkbox"/> Orders/Endorsements <input checked="" type="checkbox"/> Performance Group PG1 <input checked="" type="checkbox"/> Performance Reports PG2 <input checked="" type="checkbox"/> Commendatory Items PG3 <input checked="" type="checkbox"/> Derogatory Items PG4 <input checked="" type="checkbox"/> Sensitivity/Restrictd PG5 <input checked="" type="checkbox"/> Photographs	<input checked="" type="checkbox"/> Professional History Group PH1 <input checked="" type="checkbox"/> Promotions/Advancement PH2 <input checked="" type="checkbox"/> Service Military Education/Training PH3 <input checked="" type="checkbox"/> Civilian Education/Training PH4 <input checked="" type="checkbox"/> Service Status/Change/Revision PH5 <input checked="" type="checkbox"/> Chron Assignment History PH6 <input checked="" type="checkbox"/> Qual/License/Certificates PH7 <input checked="" type="checkbox"/> Security Access/Clearance <input checked="" type="checkbox"/> Administrative Group AG1 <input checked="" type="checkbox"/> Dependent Support/Elig AG2 <input checked="" type="checkbox"/> Personal History/Bio AG3 <input checked="" type="checkbox"/> Loan/Tuition Assistance/Elig AG4 <input checked="" type="checkbox"/> Change/Correction/Verification AG5 <input checked="" type="checkbox"/> Medical/Physical Exam/Findings AG6 <input checked="" type="checkbox"/> Miscellaneous Admin Data
--	--

SUBMIT

Figure 4-10 OMPF Request Form

4.2.2. Creating a JSRRC Request

If authorized to make JSRRC requests, click the “Create a JSRRC request” link. The JSRRC Request Form (Figure 4-11) will be displayed. Fill in the personal information (full name and Social Security Number) of the individual you are requesting records for, and select the appropriate Military Branch, Reason Code, and Station Code. A JSRRC request must contain the information for at least one of the Post-Traumatic Stress Disorder (PTSD) Stressor codes or the Agent Orange code. It can contain up to four codes if needed. To enter the request code information, select one of the request code radio buttons and then click the “Continue” link.

JSRRC REQUEST FORM

(*) - Required Field

PERSONEL INFORMATION

Social Security Number *

First Name

Last Name *

Military Branch *

Reason Code *

Station Code *

REQUEST CODES

Select an option and click the Continue button to enter JSRRC information

JSRRC Request Codes

Q40 ☐ PTSD - Stressor 1

Q41 ☐ PTSD - Stressor 2

Q42 ☐ PTSD - Stressor 3

Q43 ☐ Agent Orange Claim

CONTINUE

Figure 4-11 JSRRC Request Form

If one of the PTSD Stressor codes was selected, the PTSD Stressor form (Figure 4-12) will be displayed. Enter the mandatory information on this form and click the “Continue” button to return to the main JSRRC Request Form.

PTSD Stressor 1					
<p>** - Required Fields</p> <p>The information provided is furnished to help in identifying or reconstructing evidence to support a claim for PTSD.</p> <p>Note: This request code cannot be used for UMMC personnel. See M21-1, Part 111, Chapter 5.</p>					
Tours of Duty assignment *			Date (mm/dd/yyyy)		Stressor *
Unit Location *			From *	To *	Stressor *
					▼
					▼
					▼
Military Occupational Specialty (MOS) *					
<p>Stress-Crafting Experience ** - All information should be short and as exact as possible. If applicable, include a description of incidents concerning casualty(ies). If information is insufficient, develop for additional information prior to submission.</p>					
Cycle * (mm/dd/yyyy - If day is unknown use 01)					
Casualty(s) involved - If yes, Last Name and Status must be entered. Please supply as much of the information requested below as possible.			<input checked="" type="radio"/> Yes <input type="radio"/> No		
Last Name					
First Name					
Middle Name					
Status			▼		
<p>Unit of assignment: - If the assignment is not known, check the "Unknown". If the assignment is the same as the claimant check "Same as Tour of Duty entry". If the casualty was assigned to a different unit than the claimant, furnish the unit assignment of the casualty, if known.</p>			<input checked="" type="radio"/> Unknown <input type="radio"/> Same as Tour of Duty entry <input type="radio"/> Furnish the unit assignment of casualty <div style="border: 1px solid black; height: 20px; width: 100%; margin-top: 5px;"></div>		
<div>CONTINUE</div> <div>BACK</div>					

Figure 4-12 PTSD Stressor Form

Once the PTSD Stressor form has been completed, a red “X” appears next to the specified Request Code on the JSRRC Form (Figure 4-13). To delete an existing request, click the “X” icon and confirm the deletion when a popup message is displayed. Click the “Submit” link on the main JSRRC Request Form to complete the process of creating a JSRRC request.

The screenshot displays the 'Create Request' page for the JSRRC Request Form. At the top, there are links for 'CAMP REQUEST' and 'JSRRC REQUEST', and a date stamp '1945 Sep 20, 2011'. The form is titled 'JSRRC REQUEST FORM' and includes a section for 'PERSONNEL INFORMATION' with fields for Social Security Number, First Name, Last Name, and Military Branch (with radio button options for Air Force, Army, Coast Guard, Marine Corp, and Navy). Below this are fields for Reason Code (set to 'None') and Option Code. A section titled 'REQUEST CODES' contains a list of JSRRC Request Codes: C40 PTSD - Stressor 1 (marked with a red 'X' and a red arrow), C41 PTSD - Stressor 2, C42 PTSD - Stressor 3, and C43 Agent Orange Claim. At the bottom, there are 'CONTINUE' and 'SUBMIT' buttons, with a red arrow pointing to the 'SUBMIT' button.

Figure 4-13 JSRRC Form

If the Agent Orange code was selected, the Agent Orange Claim form (Figure 4-14) will be displayed. Enter the ship from and ship to dates for up to five shipments. Each shipment can have up to 25 pairs of dates. To add another date to a shipment (i.e., Unit assignment), click the “Add Date” button for the shipment. Once all shipment information is entered, click the “Continue” link to return to the main JSRRC Request Form.

The form is titled "Agent Orange Claim". It includes a note: "NOTE: Dates must be entered in a MM/DD/YYYY format" and "(*) : Required Field".

The form contains five sections for assignment information, each with the following fields:

- Assignment 1 Information** (and 2, 3, 4, 5 Information): (If assignment is entered, exposure circumstances and dates are mandatory)
- Unit of Assignment *
- Circumstances Surrounding Exposure to Agent Orange *
- Dates Unit Claimed Exposure to Agent Orange Occurred
- From *
- To *
- ADD DATE

At the bottom of the form, there is a red arrow pointing right with the text "CONTINUE" and a "BACK" link.

Figure 4-14 Agent Orange Claim Form

Once the appropriate selection is marked with an “X”, click “Submit” (Figure 4-15).

Figure 4-15 Submit Request Form

After successfully submitting a request, the “Your Request was submitted” page (Figure 4-16) will be shown.

Figure 4-16 Request Submitted

Once a response has been received by DPRIS, from the Service OMPF Systems of JSRRC, you will receive a notification e-mail from donotreply@dpris.org. An example of a typical system generated e-mail response is:

“This is an automated message generated by the system. PLEASE DO NOT REPLY TO THIS MESSAGE.

A response has been received for the following request:

2jL9d7G3NH4Eb7L13269_na, Smith

You may now logon to DPRIS Web and view the response to your request.”

This process typically should not take longer than 20 minutes, from the time the request has been made until the user receives a response.

4.3. VIEWING RESPONSES

At the View Responses page (Figure 4-17), which is the DPRIS default screen, click on one of the Request IDs for previously made requests.

Responses

[SIGN OUT](#)

View Responses

Retrieved 4 request(s). Displaying 10 per page.

Request ID	Last Name	SSN	Date Received	Purge days left	Extend Purge Date	Purge Request	Follow Up Message
0Xa9EdaF7jU372C9131_at	John, Roger (Don't give all)		08/2011 09:32:57	17	35 days	<input type="checkbox"/>	<input type="checkbox"/>
0Xa9EdaF7jU372C9131_ar	John, Roger (Don't give all)		08/2011 09:32:55	17	35 days	<input type="checkbox"/>	<input type="checkbox"/>
0Xa9EdaF7jU372C9131_mc	John, Roger (Don't give all)		08/2011 09:34:17	17	35 days	<input type="checkbox"/>	<input type="checkbox"/>
0Xa9EdaF7jU372C9131_na	John, Roger (Don't give all)		08/2011 09:35:41	17	35 days	<input type="checkbox"/>	<input type="checkbox"/>

Page 1 of 1

[Purge Selected Requests](#)

Quick Links

[View Subordinates' Responses](#)

Secure Area | [Privacy & Security](#)

Figure 4-17 Response IDs

In this example, a records request has already been made. The “View Subordinates' Responses” link allows a Manager to view the responses to requests initiated by their subordinates. This link will only be visible to Users who are in a managerial role and have subordinate Users. Click on the “Request ID” to begin viewing responses to requests. If no response has been received, the Request ID does not show up.

A list of available images received from the Services' OMPF repository system based on the request will be shown. Select an image to review. Then select "Display Selected Files" (Figure 4-18).

NOTE: Adobe Reader must be installed on the User's computer in order to display selected files.

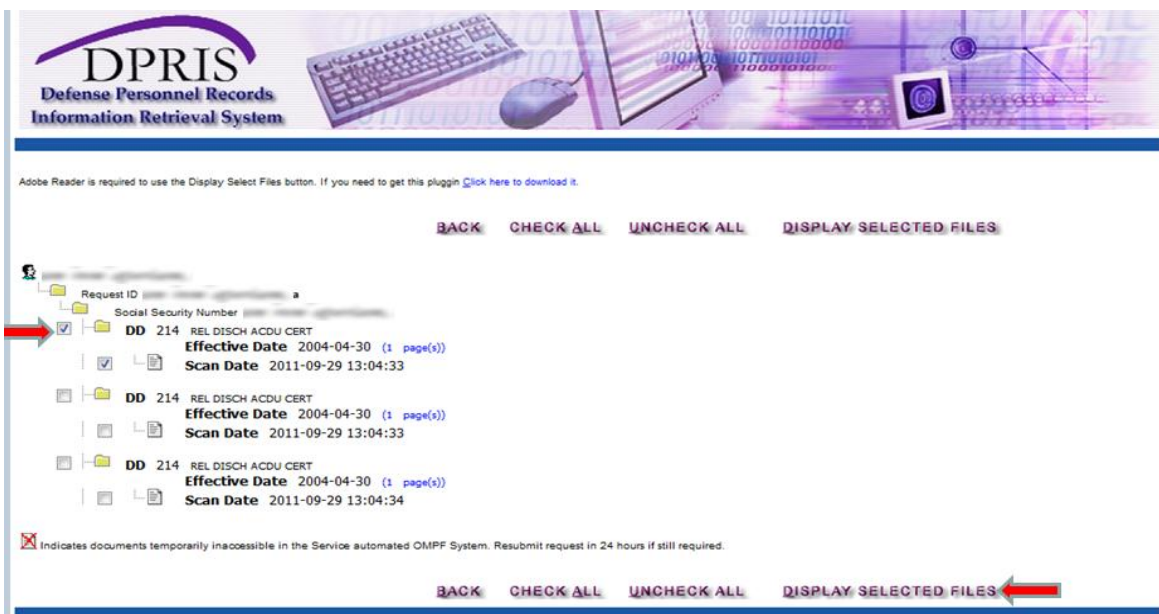


Figure 4-18 List of Available Images

Figure 4-19 shows an example of a typical form that is requested through the DPRIS system.

CAUTION: NOT TO BE USED FOR IDENTIFICATION PURPOSES		THIS IS AN IMPORTANT RECORD. SAFEGUARD IT.		ANY ALTERATIONS IN SHADED AREAS RENDER FORM VOID	
CERTIFICATE OF RELEASE OR DISCHARGE FROM ACTIVE DUTY					
1. NAME (Last, First, Middle)		2. DEPARTMENT, COMPONENT AND BRANCH		3. SOCIAL SECURITY NO.	
4.a. GRADE, RATE OR RANK		4.b. PAY GRADE		5. DATE OF BIRTH (YYMMDD)	
6. RESERVE OBLIG. TERM: DATE		Year N/A: Month Day			
7.a. PLACE OF ENTRY INTO ACTIVE DUTY		7.b. HOME OF RECORD AT TIME OF ENTRY (City and state, or complete address if known)			
8.a. LAST DUTY ASSIGNMENT AND MAJOR COMMAND		8.b. STATION WHERE SEPARATED			
9. COMMAND TO WHICH TRANSFERRED		10. SGLI COVERAGE <input type="checkbox"/> None			
NAVAL RESERVE PERSONNEL CENTER, NEW ORLEANS, LA 70149		Amount: \$250,000.00			
11. PRIMARY SPECIALTY (List number, title and years and months in specialty. List additional specialty numbers and titles involving periods of one or more years.)		12. RECORD OF SERVICE		Year(s) Month(s) Day(s)	
PNC: XXXXXXXXXXXXXXXXXXXX		a. Date Entered AD This Period		1984 APR 19	
XXXXXXXXXXXXXXXXXXXX		b. Separation Date This Period		2004 APR 30	
XXXXXXXXXXXXXXXXXXXX		c. Net Active Service This Period		20 00 12	
XXXXXXXXXXXXXXXXXXXX		d. Total Prior Active Service		00 00 00	
XXXXXXXXXXXXXXXXXXXX		e. Total Prior Inactive Service		00 08 15	
XXXXXXXXXXXXXXXXXXXX		f. Foreign Service		15 03 03	
XXXXXXXXXXXXXXXXXXXX		g. Sea Service		05 10 02	
XXXXXXXXXXXXXXXXXXXX		h. Effective Date of Pay Grade		1997 MAY 16	

Figure 4-19 DD Form 214

4.4. WEB-BASED DPRIS REPORTS

To navigate to the Reports page, click on the “Reports” link (Figure 4-20). Access to different types of Web-based reports will be found on this page. Click on each Web-based report to access the report.

NOTE: Report availability is based on user roles and access permissions determined at the manager level. Typically, only Super Users and Managers will have access to these reports.

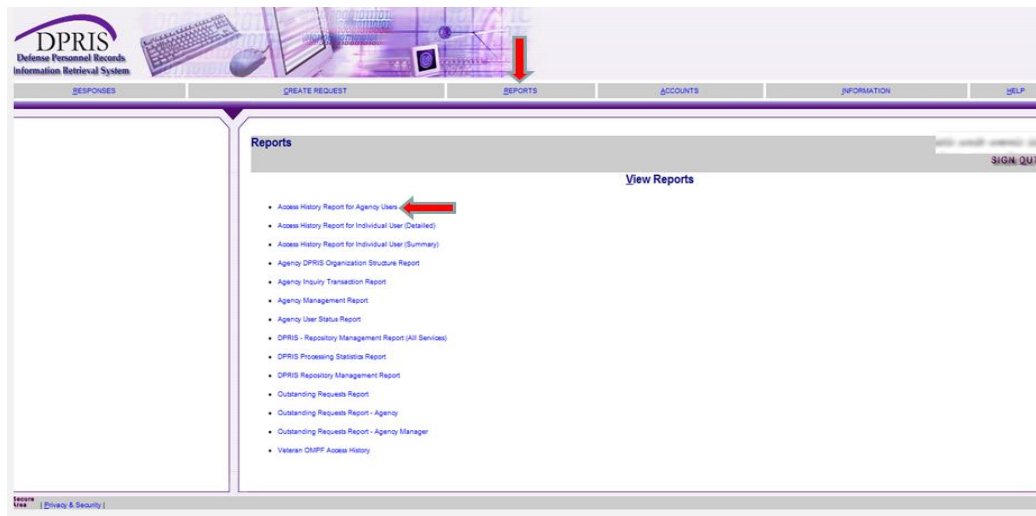


Figure 4-20 Reports Page

Figure 4-21 shows an example of an Access History Report For Agency Users.



Figure 4-21 Web-Based Report

5. ACCOUNT MANAGEMENT

Managers have the responsibility of managing DPRIS accounts for their subordinate Users through the DPRIS Web site. The roles associated with this activity are assigned as part of the User approval process and are recognized by the DPRIS system when a User logs in. Managers are authorized to approve new User registration requests, change the document assignment and authority role of their active subordinate Users, and temporarily and permanently deactivate subordinate Users. The ability to manage other User accounts is available only to Users in a managerial role.

From the DPRIS View Responses/Default Screen, click on the “Accounts” link to navigate to the Account Management page (Figure 5-1). From the Account Management page, you can access links to modify profiles, change passwords, and manage subordinate Users if applicable.

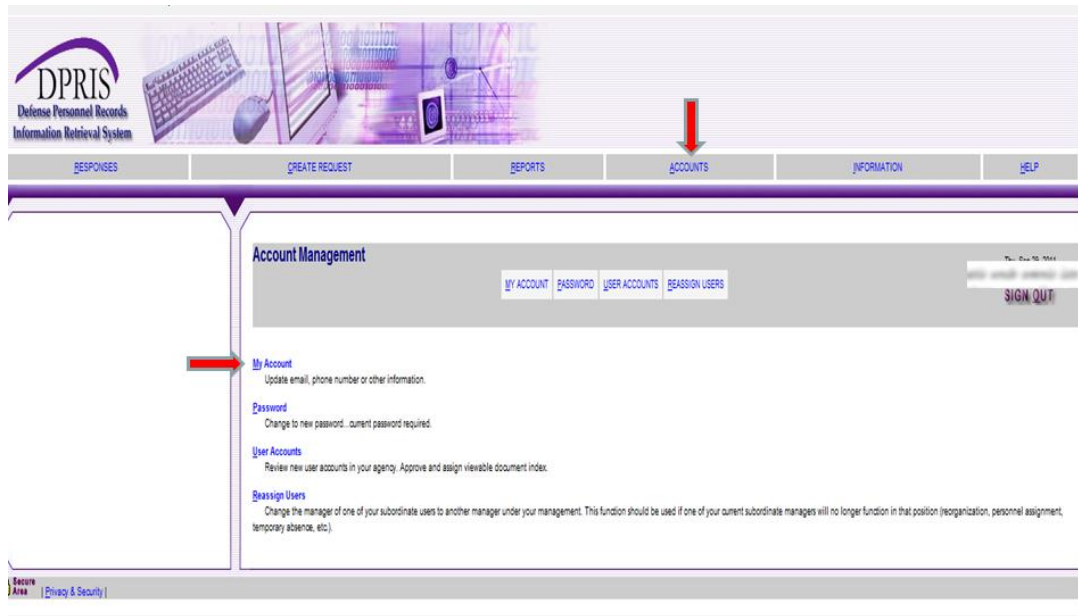


Figure 5-1 Account Management

5.1. CHANGING YOUR ACCOUNT PROFILE

As a User, you can make changes to your account portfolio, such as modifying your e-mail address, to your account profile. Click on the “My Account” link and make the appropriate changes on the “My Account” page (Figure 5-2). Click “Submit” once you have made your changes.

NOTE: Your User ID cannot be altered for any reason. If a new User ID is required, your old account needs to be deactivated by your Manager. You must then go through the registration process again with the new User ID.

DPRIS
Defense Personnel Records
Information Retrieval System

RESPONSES CREATE REQUEST REPORTS ACCOUNTS INFORMATION HELP

Account Management

MY ACCOUNT PASSWORD USER ACCOUNTS SESSION USERS

MY ACCOUNT

(*) - All fields are required

PERSONAL INFORMATION

First Name *

Middle Initial Use an alpha character (A-Z, a-d)

Last Name *

Secret Question * Choose a question only you know the answer to and that has nothing to do with your password. If you forget your password, we'll verify your identity by asking you this question.

Secret Answer * Your current answer is not being displayed for security purposes. Only enter an answer if you want to change your current one. If you do not enter an answer, your current one will not change.

Email Address *

Phone Number * Please do NOT use "-" in the phone number.

Your Office Code or Symbol

SUBMIT

Figure 5-2 My Account Profile

5.2. CHANGING YOUR PASSWORD

From the “Accounts” link in Figure 5-3, the Account Management page is displayed. Be sure to adhere to the aforementioned strong password rules in Figure 3-6 when making this change. Enter and confirm a new password then click “Submit”.

The screenshot displays the DPRIS (Defense Personnel Records Information Retrieval System) web interface. At the top, a navigation bar includes links for RESPONSES, CREATE REQUEST, REPORTS, ACCOUNTS, INFORMATION, and HELP. A red arrow points to the ACCOUNTS link. Below this, the Account Management section contains tabs for MY ACCOUNT, PASSWORD, USER ACCOUNTS, and REASSIGN USERS. A red arrow points to the PASSWORD tab. The main content area is titled "PASSWORD" and includes a note: "(*) - All fields are required". Under the heading "PASSWORD INFORMATION", there are three input fields: "Current Password *", "New Password *", and "Confirm New Password *". Each field is followed by a series of asterisks indicating masked text. To the right of these fields, a text box provides password requirements: "Passwords must be 8 characters in length and contain no spaces. Each password must contain a minimum of one upper case alpha, one lower case alpha, one numeric and one special character. [Click Here for a complete list of password rules.](#)". A red arrow points to the "Current Password *" field. At the bottom of the form, a red arrow points to the "SUBMIT" button. The footer of the page includes a "Security Alert" icon and a link to "Privacy & Security".

Figure 5-3 Changing Your Password

5.3. ACTIVATING, DEACTIVATING & REJECTING USERS

Managers are responsible for approving new User registration requests, changing the document assignment and authority role of their active Users assigned to them, and temporarily and permanently deactivating the Users assigned to them.

5.3.1. Activating New Users

Managers will receive an e-mail whenever a new User has submitted a registration form and selected them as their Manager. From the Account Management page (Figure 5-4), click on “User Accounts” and select “New Users”.

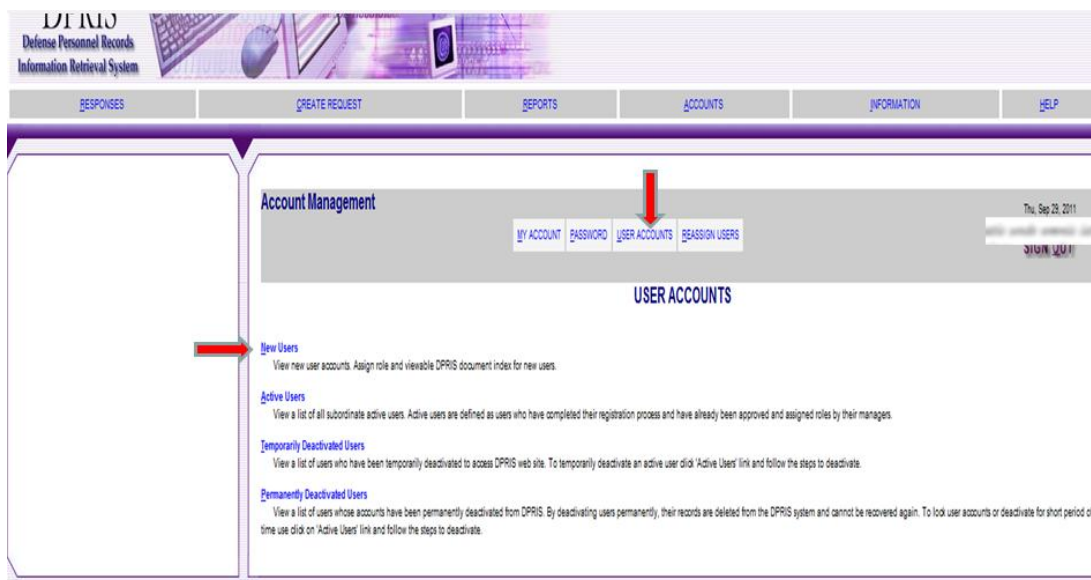


Figure 5-4 User Accounts

Click on the new User's name from the New User Accounts page (Figure 5-5).

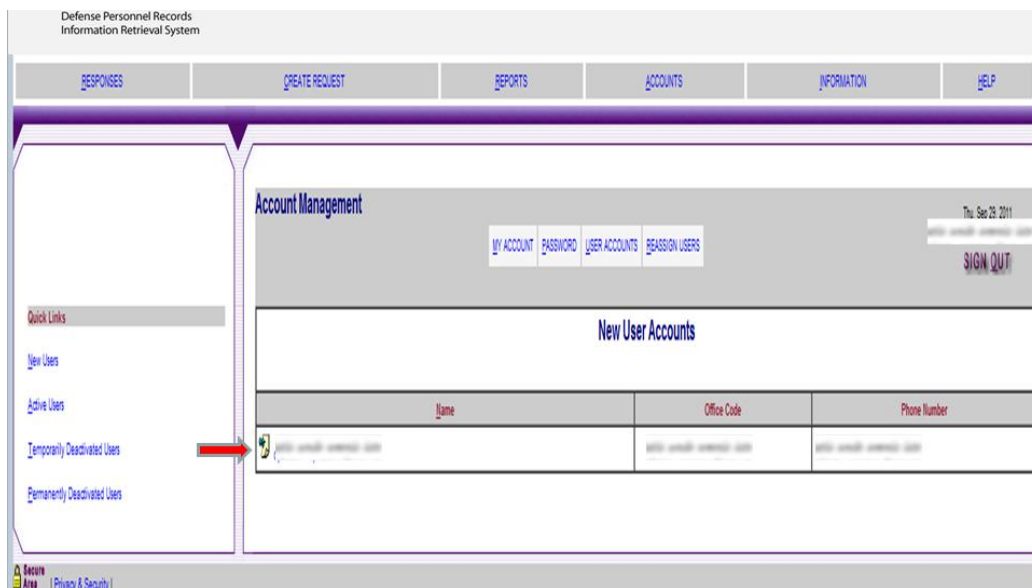


Figure 5-5 New User Account

The potential new User's Profile information page (Figure 5-6) is displayed. It is important that the information pre-populated into this form is reviewed to ensure accuracy. Once the information has been verified, click "Continue".

Account Management

MY ACCOUNT | PASSWORD | USER ACCOUNTS | SESSION USERS

Profile for [User Name]

** Please review all of the user's information carefully. If any information is incorrect, please click the Reject button on the next page.
** Please make certain the user's Email Address is correct.

PERSONAL INFORMATION

User ID	
First Name	
Middle Initial	
Last Name	
Phone Number	
Email Address (Must Be Valid)	
Login Method	

AGENCY INFORMATION

Office Code	
Manager's Name	
Manager's Phone	
Manager's Email	
Manager's Office Code	

CONTINUE

Figure 5-6 New User Profile

The Role Assignment page (Figure 5-7) is displayed. Here, the type of requests can be specified. This form is used for assignment of access. An advantage of DPRIS is that a User does not have to go through a large number of images if, for example, they only need the Service Computation Group or more specifically the DD Form 214. Only those Users with an approved business need will have JSRRC access. To approve the request, click "Activate".

Account Management

MY ACCOUNT | PASSWORD | USER ACCOUNTS | SESSION USERS

Role Assignment for [User Name]

User Role Level *

User

Website Documents *

<input checked="" type="checkbox"/> Service Computation Group SC1 <input checked="" type="checkbox"/> DD214 SC2 <input checked="" type="checkbox"/> Service Verification/Computation SC3 <input checked="" type="checkbox"/> Officer App/Termination SC4 <input checked="" type="checkbox"/> Enlistment/Extensions SC5 <input checked="" type="checkbox"/> Service Acknowledgement/Agt SC6 <input checked="" type="checkbox"/> Discharge/Separation/Ret SC7 <input checked="" type="checkbox"/> Casualty/Death SC8 <input checked="" type="checkbox"/> Orders/Endorsements <input checked="" type="checkbox"/> Performance Group PG1 <input checked="" type="checkbox"/> Performance Reports PG2 <input checked="" type="checkbox"/> Commendatory Items PG3 <input checked="" type="checkbox"/> Derogatory Items PG4 <input checked="" type="checkbox"/> Sensitive/Restricted PG5 <input checked="" type="checkbox"/> Photographs <input checked="" type="checkbox"/> JSRRC Request Codes O40 <input checked="" type="checkbox"/> PTSD - Stressor 1 O41 <input checked="" type="checkbox"/> PTSD - Stressor 2 O42 <input checked="" type="checkbox"/> PTSD - Stressor 3 O43 <input checked="" type="checkbox"/> Agent Orange Claim	<input checked="" type="checkbox"/> Professional History Group PH1 <input checked="" type="checkbox"/> Promotion/Adv/Reduction PH2 <input checked="" type="checkbox"/> Service Military Edu/Training PH3 <input checked="" type="checkbox"/> Civilian Education/Training PH4 <input checked="" type="checkbox"/> Service Status/Change/Revision PH5 <input checked="" type="checkbox"/> Chron Assignment History PH6 <input checked="" type="checkbox"/> Quals/Licensers/Certificates PH7 <input checked="" type="checkbox"/> Security Access/Clearance <input type="checkbox"/> Administrative Group AG1 <input type="checkbox"/> Dependant Support/Elig AG2 <input type="checkbox"/> Personal History/Bio AG3 <input type="checkbox"/> Loan/Tuition Assistance/Elig AG4 <input type="checkbox"/> Change/Correction/Verification AG5 <input type="checkbox"/> Medical/Physical/Exam/Findings AG6 <input type="checkbox"/> Miscellaneous Admin Docs
---	---

ACTIVATE **REJECT**

Figure 5-7 Role Assignment

5.3.2. Deactivating Users

When a User no longer requires access to DPRIS a Manager is required to deactivate the User. To do so, click on “Active Users” from the Quick Links Menu (Figure 5-8) to receive a list of all active User accounts. Click on the name of the User to deactivate the account.

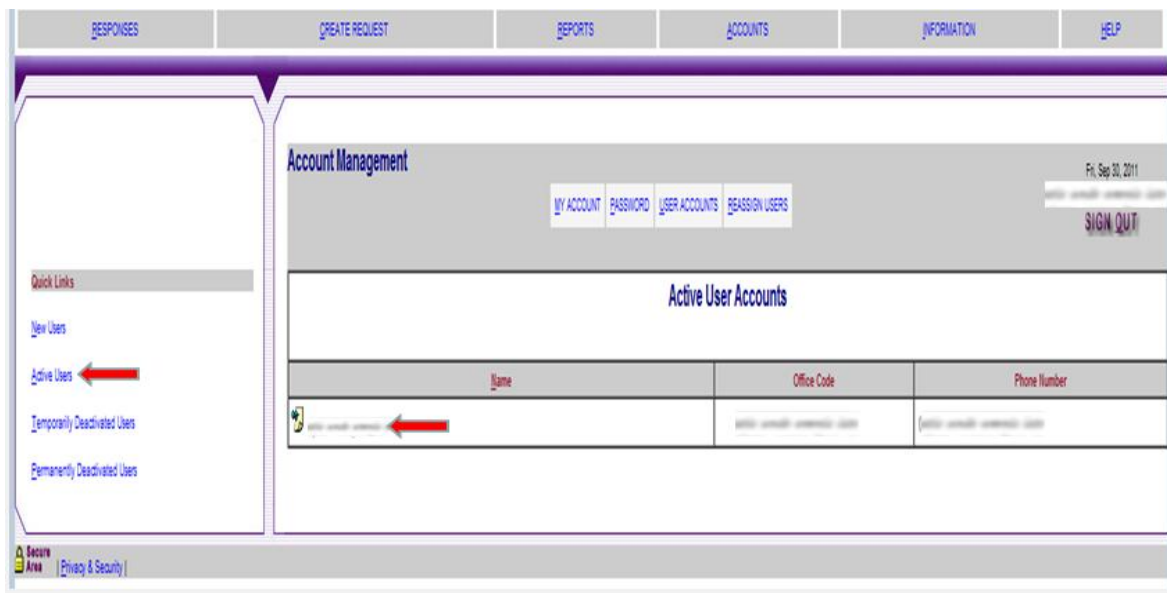


Figure 5-8 Deactivating an Active User Account

Review the User's account profile (Figure 5-9), to verify this is the User you would like to deactivate and click “Continue”.

The screenshot shows the 'Profile for' user profile page. The header includes 'Account Management' and links for MY ACCOUNT, PASSWORD, USER ACCOUNTS, and REASSIGN USERS. The profile is for a user named 'dpris_admin'. The form is divided into two sections: PERSONAL INFORMATION and AGENCY INFORMATION. The PERSONAL INFORMATION section includes fields for User ID, First Name, Middle Initial, Last Name, Phone Number, Email Address (Must Be Valid), and Login Method (USERID). The AGENCY INFORMATION section includes fields for Office Code, Manager's Name, Manager's Phone, Manager's Email, and Manager's Office Code. At the bottom, there is a 'CONTINUE' button highlighted with a red arrow.

Figure 5-9 Deactivate User Profile

The Role Assignment page (Figure 5-10) is then displayed. Click “Deactivate”.

The screenshot shows the 'Role Assignment for [User Name]' page. It features a navigation bar with links: MY ACCOUNT, PASSWORD, USER ACCOUNTS, and DEASSIGN USERS. Below the title, there's a section for 'User Role Level' with a dropdown menu set to 'User'. A 'Visible Documents' section is also present. The main area is divided into two columns of role groups, each with a list of specific roles and checkboxes. The left column includes 'Service Computation Group' (SC1-SC8), 'Performance Group' (PG1-PG5), and 'LSRRRC Request Codes' (O40-O43). The right column includes 'Professional History Group' (PH1-PH7) and 'Administrative Group' (AG1-AG6). At the bottom, there are two buttons: 'UPDATE' and 'DEACTIVATE', with a red arrow pointing to 'DEACTIVATE'.

Figure 5-10 Deactivate User

From this screen select either temporary or permanent deactivation and click “Submit” to complete the deactivation process. A comment box is provided to make a note of why the User is being deactivated. Comments describing why the User is being deactivated are required. An e-mail will be sent to the User confirming the change. A list of temporarily and permanently deactivated Users can be viewed by clicking on the appropriate link on the left of the Deactivate page (Figure 5-11).

The screenshot shows the 'Deactivate' page. It has a navigation bar with links: RESPONSES, CREATE REQUEST, REPORTS, ACCOUNTS, INFORMATION, and HELP. The main title is 'Account Management'. Below the title, there's a section for 'Deactivate' with a dropdown menu for 'Deactivation Options'. The 'Temporary' option is selected. Below this is a 'Comments' section with a text area for entering a reason. At the bottom, there is a 'SUBMIT' button with a red arrow pointing to it.

Figure 5-11 Deactivation Submission

5.3.3. Rejecting a User

If a New User Registration Form is incorrectly filled out, or there is another issue, reject the new User registration form by navigating to that User's Role Assignment page (Figure 5-12).

The screenshot shows the 'Role Assignment for' page. The page has a sidebar with 'Quick Links' including 'New Users', 'Active Users', 'Temporarily Deactivated Users', 'Permanently Deactivated Users', and 'Reset Password'. The main content area is titled 'Role Assignment for' and includes a 'User Role Level' dropdown set to 'User'. Below this is a 'Visible Documents' section. The main part of the page is a table of roles and groups with checkboxes. The roles include 'Service Computation Group', 'Performance Group', 'DMRC Request Codes', and 'Professional History Group'. The groups include 'Performance Reports', 'Commentary Items', 'Derogatory Items', 'Sensitive/Restricted', 'Photographs', 'Promotion/Adv/Reduction', 'Service Military Edu/Training', 'Civilian Education/Training', 'Service Status/Change/Revision', 'Chron Assignment History', 'Quals/Licenses/Certificates', 'Security Access/Clearance', 'Administrative Group', 'Dependant Support/Elig', 'Personal History/Bio', 'Loan/Tuition Assistance/Elig', 'Change/Correction/Verification', 'Medical/Physical Exam Findings', and 'Miscellaneous Admin Docs'. At the bottom right, there are 'ACTIVATE' and 'REJECT' buttons, with a red arrow pointing to the 'REJECT' button.

Figure 5-12 Rejecting a User

Select the reason that best describes why the request has been rejected on the Reject Authorization page (Figure 5-13). There is a section for comments, which will go to the User in an e-mail. Once completed, click "Submit". User registrations that are rejected are completely purged from the system, and the User is required to begin the registration process again.

The screenshot shows the 'Reject Authorization for' page. The page has a sidebar with 'Quick Links' including 'New Users', 'Active Users', 'Temporarily Deactivated Users', 'Permanently Deactivated Users', and 'Reset Password'. The main content area is titled 'Reject Authorization for'. It includes a 'Rejection Reasons' section with radio buttons for 'Modification required to user's personal information', 'Modification required to user's agency information', 'User does not belong to your agency', 'User registered with incorrect User ID', 'User registered with wrong login method', and 'Other'. Below this is a 'Comments' section with a text area for entering a reason for rejecting the case. At the bottom right, there is a 'SUBMIT' button, with a red arrow pointing to it.

Figure 5-13 Reject Authorization

5.4. UPDATING USER PROFILES

Managers can change a User's role level and/or modify the viewable documents that the User has access to. To update a subordinate User's profile, the Manager should navigate to that User's Role Assignment page (Figure 5-14) and check or un-check the desired boxes to change that User's viewable documents and then click "Update".

MY ACCOUNT | PASSWORD | USER ACCOUNTS | **REASSIGN USERS**

Role Assignment for [User Name]

User Role Level *

User

Viewable Documents *

<input checked="" type="checkbox"/> Service Computation Group SC1 <input checked="" type="checkbox"/> DD214 SC2 <input checked="" type="checkbox"/> Service Verification/Computation SC3 <input checked="" type="checkbox"/> Officer Appt/Termination SC4 <input checked="" type="checkbox"/> Enlistment/Extensions SC5 <input checked="" type="checkbox"/> Service Acknowledgement/Agt SC6 <input checked="" type="checkbox"/> Discharge/Separation/Ret SC7 <input checked="" type="checkbox"/> Casualty/Death SC8 <input checked="" type="checkbox"/> Orders/Endorsements <input checked="" type="checkbox"/> Performance Group PG1 <input checked="" type="checkbox"/> Performance Reports PG2 <input checked="" type="checkbox"/> Commendatory Items PG3 <input checked="" type="checkbox"/> Derogatory Items PG4 <input checked="" type="checkbox"/> Sensitive/Restricted PG5 <input checked="" type="checkbox"/> Photographs <input checked="" type="checkbox"/> SRRC Request Codes O40 <input checked="" type="checkbox"/> PTSD - Stressor 1 O41 <input checked="" type="checkbox"/> PTSD - Stressor 2 O42 <input checked="" type="checkbox"/> PTSD - Stressor 3 O43 <input checked="" type="checkbox"/> Agent Orange Claim	<input checked="" type="checkbox"/> Professional History Group PH1 <input checked="" type="checkbox"/> Promotion/Adv/Reduction PH2 <input checked="" type="checkbox"/> Service Military Educ/Training PH3 <input checked="" type="checkbox"/> Civilian Education/Training PH4 <input checked="" type="checkbox"/> Service Status/Change/Revision PH5 <input checked="" type="checkbox"/> Chron Assignment History PH6 <input checked="" type="checkbox"/> Quals/Licenses/Certificates PH7 <input checked="" type="checkbox"/> Security Access/Clearance <input type="checkbox"/> Administrative Group AG1 <input type="checkbox"/> Dependant Support/Elig AG2 <input type="checkbox"/> Personal History/Bio AG3 <input type="checkbox"/> Loan/Tuition Assistance/Elig AG4 <input type="checkbox"/> Change/Correction/Verification AG5 <input type="checkbox"/> Medical/Physical/Exam/Findings AG6 <input type="checkbox"/> Miscellaneous Admin Docs
---	---

UPDATE **REACTIVATE**

Figure 5-14 Updating User Profiles

5.5. FORGOTTEN PASSWORDS

5.5.1. Resetting Your Password

If you forget your password it can be reset. However, after three unsuccessful login attempts, you will be locked out of DPRIS and the Number of Invalid Login Attempts Exceeded page (Figure 5-15) will appear. If this screen appears, the password must then be reset by the User's Manager.

NOTE: User ID, password, and security challenge answers are all case-sensitive – must be exact.

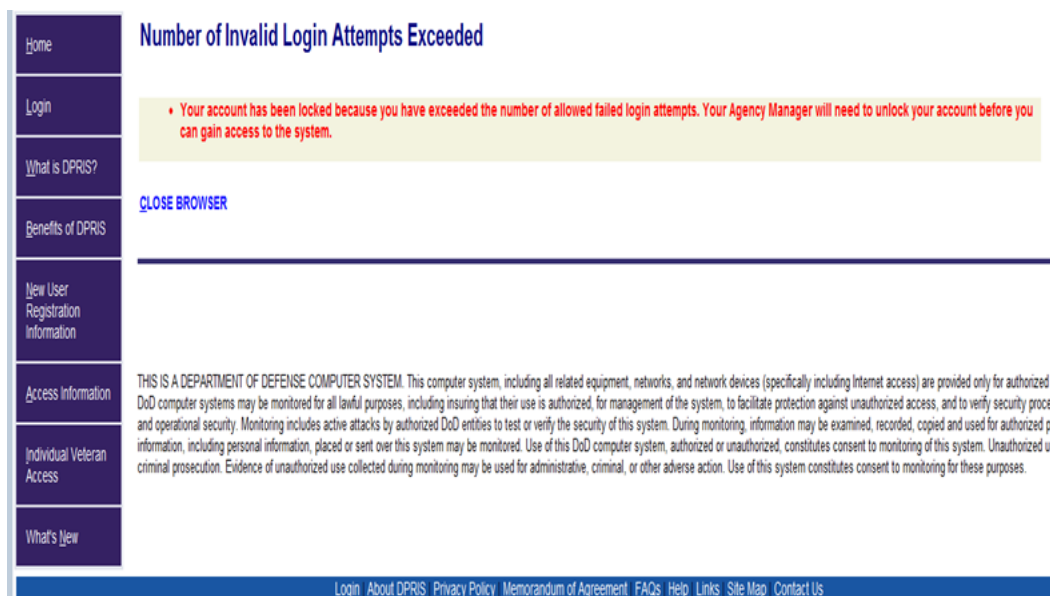


Figure 5-15 Invalid Login Attempts

To reset your password, click on the “Forgot Password” link on the DPRIS Home page (Figure 5-16).

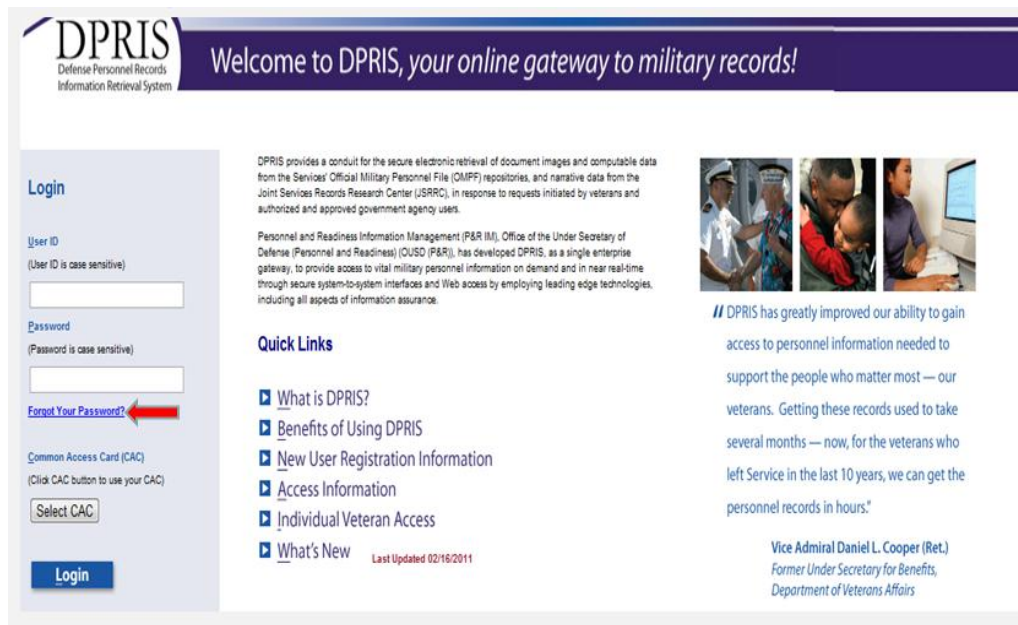


Figure 5-16 Forgot Your Password

At the DPRIS Forgotten Password page (Figure 5-17), enter your User ID and e-mail address. If both are entered correctly your secret question (you selected your secret question when you initially registered) will be displayed. An e-mail with your password will be sent to you. During your next login, a new password will be required.

(NOTE: Please keep in mind that the new User password must adhere to the password rules defined in aforementioned Figure 3-6.)

Figure 5-17 Forgot Password Prompt

5.5.2. Resetting Another User's Password

If a User has forgotten their password and is locked out of their account, the password can be reset by the User's Manager or Super User. The Manager or Super User will navigate to the Accounts Management page (Figure 5-18) and click on "Active Users". A list of active Users will be displayed. Select the User you would like to reset the password for by clicking on the User's name.

Figure 5-18 Resetting Another User's Password

The User's profile page will be displayed. Click the "Reset Password" link (Figure 5-19) on the left side of the screen.

Account Management

MY ACCOUNT | PASSWORD | USER ACCOUNTS | REASSIGN USERS

Profile for [redacted]

PERSONAL INFORMATION

User ID	dpris_admin
First Name	[redacted]
Middle Initial	[redacted]
Last Name	[redacted]
Phone Number	[redacted]
Email Address (Must Be Valid)	[redacted]
Login Method	USERID

AGENCY INFORMATION

Office Code	[redacted]
Manager's Name	[redacted]
Manager's Phone	[redacted]
Manager's Email	[redacted]
Manager's Office Code	[redacted]

CONTINUE

Figure 5-19 Reset Password Link

Click "Submit" (Figure 5-20).

Account Management

MY ACCOUNT | PASSWORD | USER ACCOUNTS | REASSIGN USERS

Reset Password for [redacted]

(*) - All fields are required

PASSWORD INFORMATION

New Password *	*****
Confirm New Password *	*****

SUBMIT

Figure 5-20 Submit Reset Password

NOTE: Please keep in mind that the new User password must adhere to the password rules defined in Figure 3-6.

A system generated e-mail is then sent to the User notifying them that they may log back in using their new password and that they must immediately reset their password upon logging back in. Only after this new password has been created, can they resume use of the DPRIS system.

5.6. REASSIGNING SUBORDINATE DPRIS USERS

Managers and Super Users have the ability to reassign their subordinate Users to another Manager. This is useful for when a Manager is going to be out of the office, leaves an agency, or changes projects.

Click the “Reassign Users” link on the Account Management page (Figure 5-21).

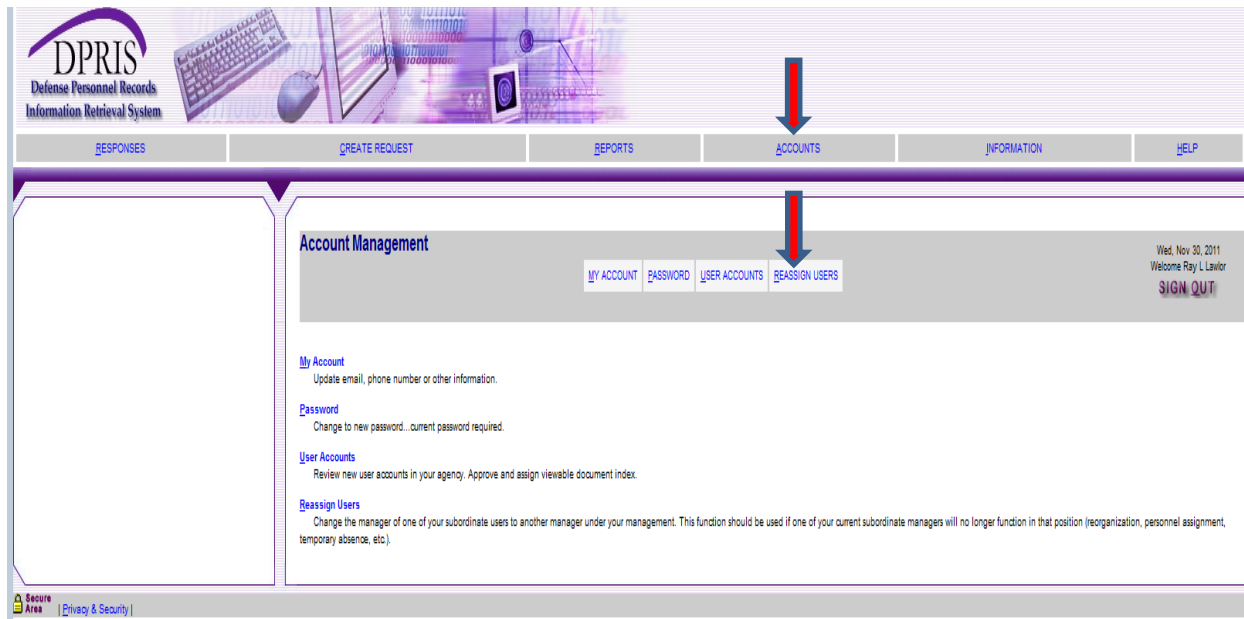


Figure 5-21 Reassign Users

A list of the subordinate Users will be displayed. Select the User(s) to be reassigned by clicking the check box on the left (Figure 5-22). Click “Continue”.

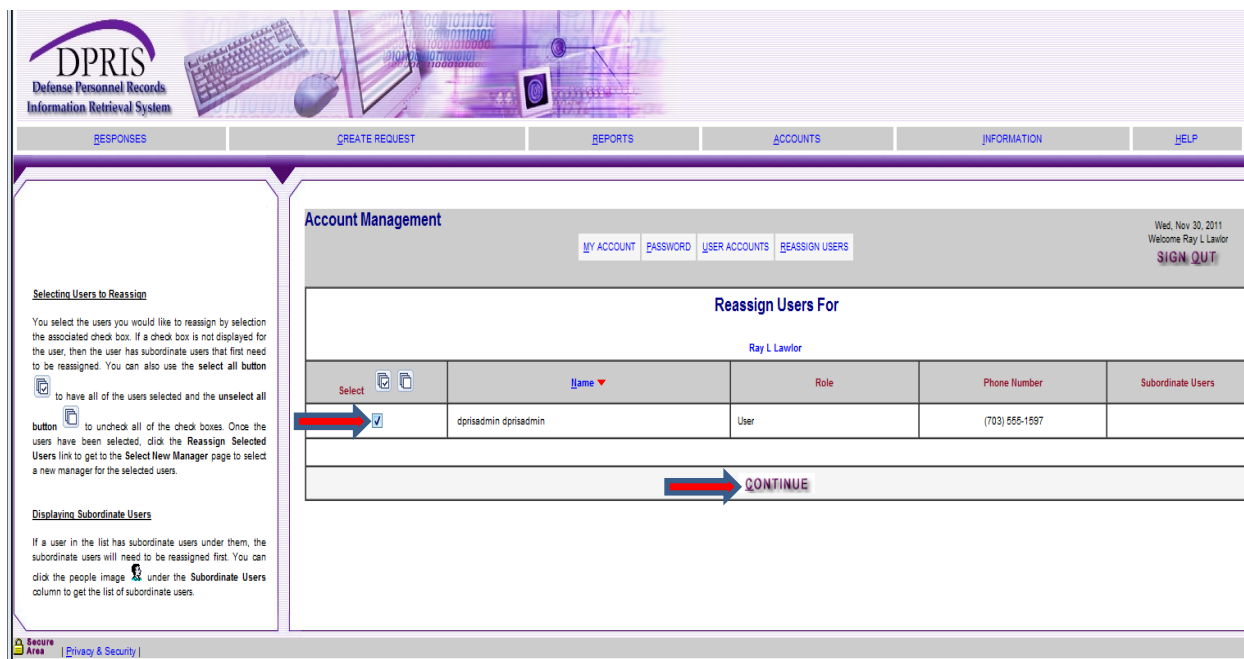


Figure 5-22 Select User to Reassign

The Select New Manager page is displayed (Figure 5-23). Click the check box next to the new Manager's name. Click "Submit" to complete the reassignment.

Account Management

MY ACCOUNT | PASSWORD | USER ACCOUNTS | REASSIGN USERS

Wed, Nov 30, 2011
Welcome Ray L Lawlor
[SIGN OUT](#)

Select New Manager

Users selected to be reassigned from Ray L Lawlor

Name	Role	Phone Number
dprisadmin dprisadmin	User	(703) 655-1597

Select a new manager for the selected users

Select *	Name	Role	Phone Number
<input checked="" type="checkbox"/>	Thomas F Darcey	Manager	(703) 696-1967
<input type="checkbox"/>	Benjamin H DeVore	Manager	(703) 845-3915
<input type="checkbox"/>	David Hong	Manager	(571) 345-4454
<input type="checkbox"/>	Thomas F Klein	Manager	(717) 540-9310
<input type="checkbox"/>	Ray L Lawlor	Manager	(703) 989-1851
<input type="checkbox"/>	matthew leach	Manager	(703) 687-7065
<input type="checkbox"/>	Jon Lee	Manager	(703) 845-3900
<input type="checkbox"/>	Eric A Lonnert	Manager	(571) 527-7824
<input type="checkbox"/>	Ellen Sulewzyki	Manager	(703) 696-1961
<input type="checkbox"/>	Michael Vogan	Super User	(703) 696-2357
<input type="checkbox"/>	Seth S Watson	Manager	(703) 377-4703

[SUBMIT](#) [BACK](#)

Choosing a New Manager for Selected Users

You select a new manager for the selected users by clicking the associated radio button. Note only one new manager can be selected. Once the new manager has been selected, click the Submit button to reassign the indicated users to the new manager selected. You also have the option to return to the previous page without making any changes.

Figure 5-23 Select New Manager

The following screen will appear (Figure 5-24).

Account Management

MY ACCOUNT | PASSWORD | USER ACCOUNTS | REASSIGN USERS

Wed, Nov 30, 2011
Welcome Ray L Lawlor
[SIGN OUT](#)

Users Reassigned Successfully!

The users selected have been successfully assigned from Ray L Lawlor to Ray Lawlor.

[BACK](#)

[Secure Area](#) | [Privacy & Security](#)

Figure 5-24 Successful Reassignment

6. INFORMATION PAGE

The DPRIS Information page (Figure 6-1) provides additional information to the User about DPRIS.



Figure 6-1 Information Page

7. DPRIS HELP

Click on the “Help” link to display the Help page (Figure 7-1).

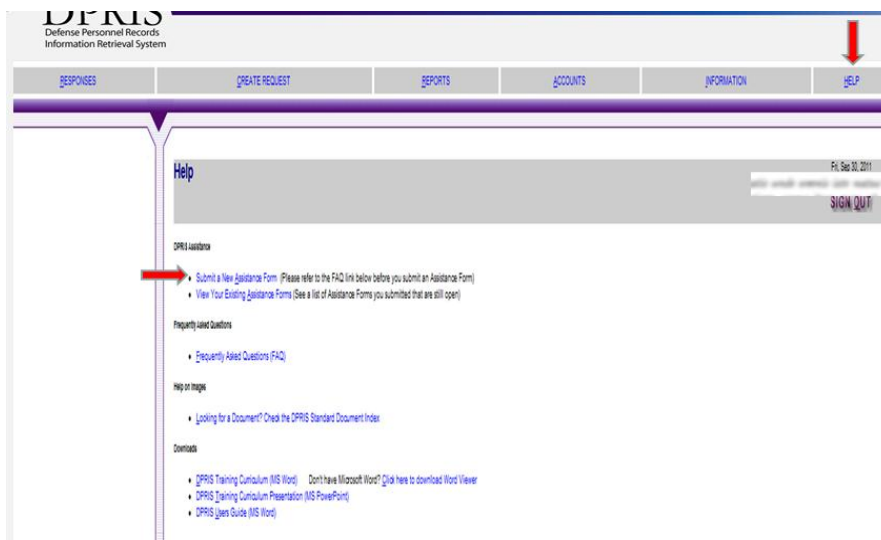


Figure 7-1 DPRIS Help

A Manager is the best resource to assist in helping a User with any questions. If the Manager is unable to fix the issue, navigate to the DPRIS Assistance Form (Figure 7-2). All Assistance Form comments are reviewed by a DPRIS functional analyst or a technical analyst. An acknowledgement of receipt and initial disposition action for suggestions, complaints, or problems/questions that do not require immediate assistance will be provided by e-mail within five working days. If your problem / question is more severe, you will receive a response by e-mail within one business day.

Figure 7-2 Assistance Form

Answers to common questions can be found on the Frequently Asked Questions page (Figure 7-3).

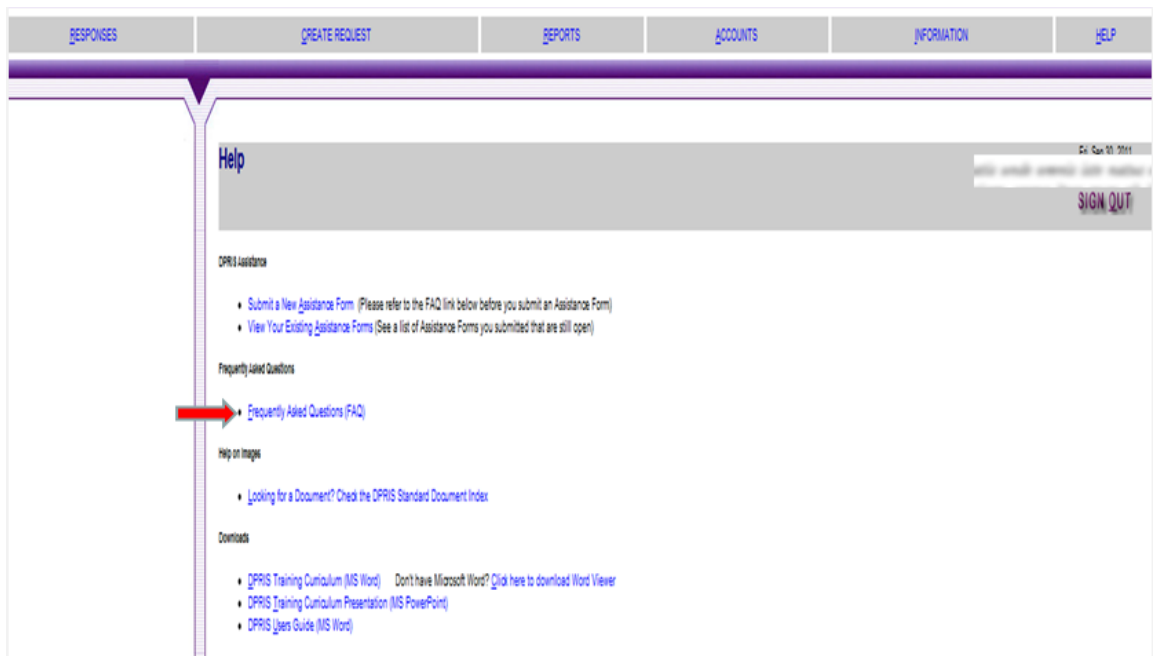


Figure 7-3 Frequently Asked Questions

8. CONCLUSION

The DPRIS Web site User Guide will be updated periodically and the most recent version will be available online via the DPRIS Web site.

APPENDIX A. ACRONYMS

The table in Appendix A shows the list of acronyms used within the User Guide.

Term	Definition
CAC	Common Access Card
DPRIS	Defense Personnel Records Information Retrieval System
HIPPA	Health Insurance Portability and Accountability Act
JSRRC	Joint Services Records Research Center
NPRC	National Personnel Records Center
OMPF	Official Military Personnel File
PIN	Personal Identification Number
PM	Program Manager
PMO	Program Management Office
PTSD	Post-Traumatic Stress Disorder